Minería de procesos aplicados a la ciberseguridad relacionados con incidentes de ataques en una empresa que ofrece el servicio de acceso a internet utilizando la herramienta ProM, enmarcado en el estándar ISO-27000

Garaicoa Martínez, Boris Alcides

Vicerrectorado Académico General

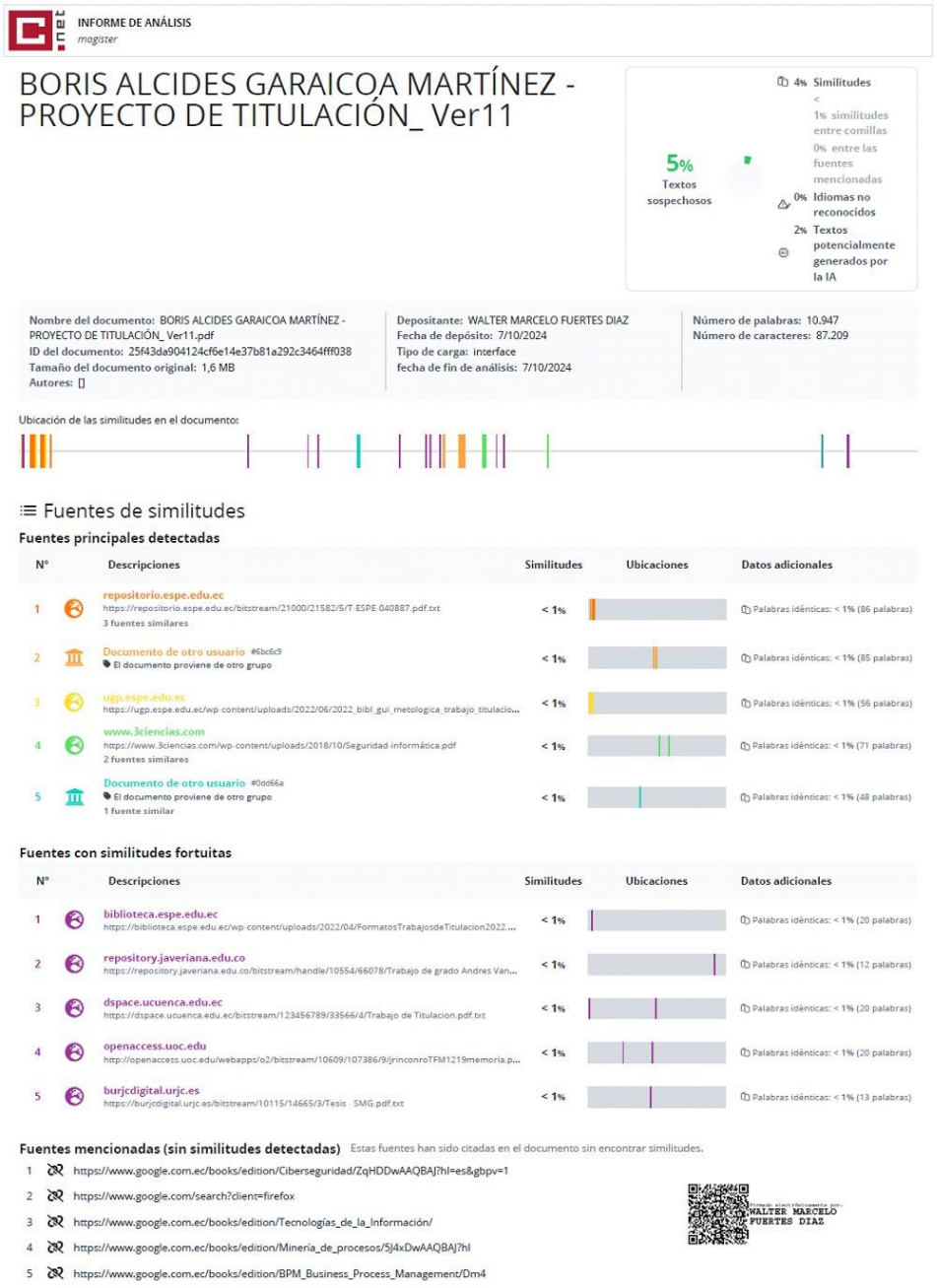
Centro de Posgrados

Maestría en Gerencia de Sistemas

Trabajo de titulación, previo a la obtención del título de Magíster en Gerencia de Sistemas

Ing. Fuertes Díaz, Walter Marcelo, PhD

25 de julio de 2025



INFORME DE ANÁLISIS
magister

BORIS ALCIDES GARAICOA MARTÍNEZ - PROYECTO DE TITULACIÓN_ Ver11

5% Textos sospechosos

4% Similitudes
< 1% similitudes entre comillas
0% entre las fuentes mencionadas
0% Idiomas no reconocidos
2% Textos potencialmente generados por la IA

Nombre del documento: BORIS ALCIDES GARAICOA MARTÍNEZ - PROYECTO DE TITULACIÓN_ Ver11.pdf
ID del documento: 25f43da904124cf6e14e37b81a292c3464fff038
Tamaño del documento original: 1,6 MB
Autores: []

Depositante: WALTER MARCELO FUERTES DIAZ
Fecha de depósito: 7/10/2024
Tipo de carga: interface
fecha de fin de análisis: 7/10/2024

Número de palabras: 10.947
Número de caracteres: 87.209

Ubicación de las similitudes en el documento:

Fuentes de similitudes

Fuentes principales detectadas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	repositorio.espe.edu.ec https://repositorio.espe.edu.ec/bitstream/21000/21582/5/T-ESPE-040887.pdf.txt 3 fuentes similares	< 1%		Palabras idénticas: < 1% (86 palabras)
2	Documento de otro usuario #6bc6c9 El documento proviene de otro grupo	< 1%		Palabras idénticas: < 1% (85 palabras)
3	ugp.espe.edu.ec https://ugp.espe.edu.ec/wp-content/uploads/2022/06/2022_bibl_gui_metologica_trabajo_titulacio...	< 1%		Palabras idénticas: < 1% (56 palabras)
4	www.3ciencias.com https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informática.pdf 2 fuentes similares	< 1%		Palabras idénticas: < 1% (71 palabras)
5	Documento de otro usuario #0dd66a El documento proviene de otro grupo 1 fuente similar	< 1%		Palabras idénticas: < 1% (48 palabras)

Fuentes con similitudes fortuitas

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	biblioteca.espe.edu.ec https://biblioteca.espe.edu.ec/wp-content/uploads/2022/04/FormatosTrabajosdeTitulacion2022....	< 1%		Palabras idénticas: < 1% (20 palabras)
2	repository.javeriana.edu.co https://repository.javeriana.edu.co/bitstream/handle/10554/66078/Trabajo de grado Andres Van...	< 1%		Palabras idénticas: < 1% (12 palabras)
3	dspace.ucuenca.edu.ec https://dspace.ucuenca.edu.ec/bitstream/123456789/33566/4/Trabajo de Titulacion.pdf.txt	< 1%		Palabras idénticas: < 1% (20 palabras)
4	openaccess.uoc.edu http://openaccess.uoc.edu/webapps/o2/bitstream/10609/107386/9/jrinconroTFM1219memoria.p...	< 1%		Palabras idénticas: < 1% (20 palabras)
5	burjcdigital.urjc.es https://burjcdigital.urjc.es/bitstream/10115/14665/3/Tesis - SMG.pdf.txt	< 1%		Palabras idénticas: < 1% (13 palabras)

Fuentes mencionadas (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://www.google.com.ec/books/edition/Ciberseguridad/ZqHDDwAAQBAJ?hl=es&gbpv=1
2 https://www.google.com/search?client=firefox
3 https://www.google.com.ec/books/edition/Tecnologías_de_la_Información/
4 https://www.google.com.ec/books/edition/Minería_de_procesos/5J4xDwAAQBAJ?hl
5 https://www.google.com.ec/books/edition/BPM_Business_Process_Management/Dm4

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
WALTER MARCELO FUERTES DIAZ

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
WALTER MARCELO FUERTES DIAZ

Ing. Fuertes Diaz, Walter Marcelo, PhD

Director

Vicerrectorado Académico General

Centro de Posgrados

Certificación

Certifico que el trabajo de titulación: "**Minería de procesos aplicados a la ciberseguridad relacionados con incidentes de ataques en una empresa que ofrece el servicio de acceso a internet utilizando la herramienta ProM, enmarcado en el estándar ISO-27000**" fue realizado por el señor **Garaicoa Martínez, Boris Alcides;** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizado en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 25 de julio de 2025

Walter Marcelo Fuertes Diaz
Time Stamping Security Data

Ing. Fuertes Diaz, Walter Marcelo, PhD

Director

C.C.: 1707017701

Vicerrectorado Académico General

Centro de Posgrados

Responsabilidad de Autoría

Yo, **Garaicoa Martínez, Boris Alcides** con cédula de ciudadanía N° 0916864861, declaro que el contenido, ideas y criterios del trabajo de titulación: **"Minería de procesos aplicados a la ciberseguridad relacionados con incidentes de ataques en una empresa que ofrece el servicio de acceso a internet utilizando la herramienta ProM, enmarcado en el estándar ISO-27000"** es de mí/nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 25 de julio de 2025

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
BORIS ALCIDES
GARAICOA MARTINEZ

Ing. Garaicoa Martínez, Boris Alcides

C.C.: 0916864861

Vicerrectorado Académico General

Centro de Posgrados

Autorización de Publicación

Yo, **Garaicoa Martínez, Boris Alcides** con cédula de ciudadanía N° 0916864861, autorizo a la Universidad de las Fuerzas Armadas ESPE, publicar el trabajo de titulación: **"Minería de procesos aplicados a la ciberseguridad relacionados con incidentes de ataques en una empresa que ofrece el servicio de acceso a internet utilizando la herramienta ProM, enmarcado en el estándar ISO-27000"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mí/nuestra responsabilidad.

Sangolquí, 25 de julio de 2025

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
BORIS ALCIDES
GARAICOA MARTINEZ

Ing. Garaicoa Martínez, Boris Alcides

C.C.: 0916864861

Dedicatoria

Dedicado:

A Dios Padre y a su hijo Jesucristo; por darme la vida y su guía en todo momento.

A mi amada esposa y a mis hijos por su paciencia y cariño a lo largo de mi carrera.

A mi madre y hermanas, quienes siempre me infundieron fe y ánimos para seguir adelante.

Boris Alcides Garaicoa Martínez

Agradecimiento

Al Ing. Walter Fuertes por su paciencia, guía y dedicación en el desarrollo de este trabajo, por compartir sus experiencias y conocimientos

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

Este proyecto se enfocó en la minería de procesos relacionados con la seguridad de la información. El objetivo fue realizar una Minería de Procesos aplicados a la ciberseguridad relacionados con incidentes de ataques en una empresa que ofrece el Servicio de Acceso a Internet utilizando la herramienta ProM, enmarcado en el estándar ISO-27000. La minería de procesos se llevará a cabo utilizando la metodología ProM. La investigación se enfocará en una empresa que ofrece servicios de acceso a internet. Aunque tanto los usuarios como los proveedores de servicios son conscientes de la importancia de la seguridad de la información, los proveedores hacen esfuerzos para minimizar las amenazas. Sin embargo, las estrategias implementadas no siempre están alineadas con una norma internacional. Por eso, la minería de procesos propuesta se basará en el estándar ISO-27001, lo que permitirá una mejor aplicación de las estrategias mencionadas. Para los proveedores de servicios de acceso a internet, es crucial minimizar los impactos de los ataques informáticos. Sin embargo, no cuentan con procesos específicos para reducir estos impactos. Por ello, es necesario establecer procesos prácticos basados en una normativa internacional. El modelado para descubrir, mejorar y controlar procesos se convierte en una herramienta esencial para la toma de decisiones en todos los niveles de gestión.

Palabras clave: ciberseguridad, minería de datos, ataques Informáticos, minería de procesos

Abstract

This project focused on data mining related to information security. The objective was to perform process mining applied to cybersecurity—specifically regarding attack incidents—at a company that provides Internet access services, using the ProM tool and in accordance with the ISO 27000 standard. The process mining will be carried out using the ProM methodology. The research will focus on a company that provides internet access services. Although both users and service providers are aware of the importance of information security, providers make efforts to minimize threats. However, the strategies implemented are not always aligned with an international standard. Therefore, the proposed process mining will be based on the ISO-27001 standard, which will allow for better implementation of the aforementioned strategies. For internet access service providers, it is crucial to minimize the impacts of cyberattacks. However, they lack specific processes to reduce these impacts. Therefore, it is necessary to establish practical processes based on an international standard. Modeling to discover, improve, and control processes becomes an essential tool for decision-making at all management levels.

Keywords: cybersecurity, data mining, computer attacks, process mining

Capítulo I

El problema de la investigación

Introducción

La ciberseguridad se refiere al uso seguro y responsable de los productos de tecnología de la información y comunicación (TIC), como internet, dispositivos móviles y otros instrumentos tecnológicos diseñados para almacenar, compartir o recibir información, como teléfonos móviles y cámaras digitales (Giant, 2017).

Los proveedores de servicios de acceso a internet no cuentan con procesos específicos para controlar ataques cibernéticos, y si los tienen, no siguen recomendaciones estandarizadas. Por ello, es necesario establecer procesos válidos que permitan crear políticas efectivas ante posibles eventos delictivos relacionados con la información. La minería de procesos es una herramienta valiosa para que una organización pueda realizar sus operaciones de manera segura. Estos procesos deben estar alineados con parámetros legales y administrativos, como el estándar ISO-27000, para ser prácticos.

La serie de normas ISO/IEC 27000 ha sido desarrollada para proporcionar prácticas recomendadas en seguridad de la información, con el fin de desarrollar, implementar y mantener sistemas de gestión de la seguridad de la información (SGSI) (Raya, 2020, pág. 29).

Esta investigación se centra en la falta de control integral en el manejo de datos operativos relacionados con la ciberseguridad en una empresa de servicios de internet en la Ciudad de Milagro. La carencia de ciberseguridad genera un alto nivel de ataques cibernéticos, lo que afecta negativamente la calidad del servicio ofrecido a los usuarios.

La falta de políticas y normas dentro del plan estratégico de la empresa genera inseguridad en la ejecución de los procesos operacionales, ralentizando la mitigación de la inseguridad cibernética. Además, la ausencia de un sistema de procesos basado en normas legales vigentes provoca ineficiencia en el control y manejo de los datos proporcionados en el servicio de internet.

Objetivos de la investigación

Objetivo general

Realizar una Minería de Procesos aplicados a la ciberseguridad relacionados con incidentes de ataques en una empresa que ofrece el Servicio de Acceso a Internet utilizando la herramienta ProM, enmarcado en el estándar ISO-27000.

Objetivos específicos

- Analizar la calidad de servicio de internet brindada a los usuarios, con el fin de determinar la necesidad de implementar una adecuada ciberseguridad dentro de la empresa.
- Analizar el nivel de riesgo en los procesos operacionales en cuanto a la seguridad cibernética.
- Determinar el grado de cumplimiento de normas legales en el control y seguridad de los procesos basándose en la norma ISO 27001.

Problema central

¿Qué ocasiona la inexistencia de un control integral en el proceso secuencial del manejo de los datos operativos relacionados a la ciberseguridad de una empresa que ofrece servicio de internet?

Problemas derivados

¿Qué genera la carencia de ciberseguridad en la calidad del servicio brindado a los usuarios?

¿Qué produce la falta de seguridad en los procesos operacionales gestionados en el servicio de internet con respecto a la seguridad cibernética?

¿Qué ocasiona el no contar con un sistema de procesos basados en las normas legales y vigentes en los datos proporcionados en el servicio de internet?

Justificación

Se vive en la actualidad en un mundo modernizado y totalmente globalizado, donde la tecnología y sus avances, cada día se expanden más, las tecnologías en el uso de la información no se quedan atrás, son cada vez más las técnicas tecnológicas y descubrimientos al alcance de las personas.

El uso del internet en la actualidad es una herramienta de total dependencia por parte de los seres humanos, se utiliza en casi todos los ámbitos, ya sean estos, empresariales, sociales, educativos, salud, etc. Pero a través del tiempo y de esta asombrosa evolución tecnológica, también se han presentado inconvenientes en el uso de la información y el procesamiento de datos a través de los canales de distribución del internet, son cada vez más numerosas, las empresas dedicadas a ofrecer este servicio tan indispensable de manera general.

Sin embargo, la seguridad con la que se propaga la información y los datos manejados a través de ella, han presentado inconvenientes, la existencia de virus tecnológicos en las páginas web, contaminan no solamente la información sino también los medios electrónicos en los cuales se plasma dicha información; esta también el plagio de redes informáticas, la inseguridad cibernética. Es tan masiva la cantidad de información que interfiere en los canales de distribución y uso del internet, que el peligro es inminente.

Existen normas y estatutos legales que ayudan con la mitigación de los problemas de ciberseguridad en la actualidad, es por esto que la presente investigación busca aportar de manera positiva y significativa a la expansión de datos y a la seguridad de los mismos, a través de métodos y parámetros que conlleven a una factible solución ante la ciberseguridad, Es posible implementar herramientas como la minería de procesos utilizando ProM para esta finalidad, así también que estos estén basados en estándares que permitan agregar valor a la operación de la organización.

Estado del arte

Para esta línea de investigación, se tomaron como referencia varios trabajos bien fundamentados:

En Ecuador, Chamorro Sangoquiza (2019), en su estudio “Estudio comparativo de Técnicas de minería de datos para develar patrones de desempeño académico en enseñanza media”, menciona que la cantidad de datos a nivel mundial sigue aumentando con la digitalización de la información. Esto hace que sea cada vez más difícil para las personas obtener información relevante, ya que los datos se vuelven menos comprensibles y rara vez se aprovechan adecuadamente. Por lo tanto, surge la necesidad de utilizar métodos automatizados de procesamiento de datos para descubrir los patrones subyacentes.

En España, González Escobosa (2016), en su investigación “Minería de procesos en ambientes sensorizados”, señala que la minería de procesos ha tenido poca acogida, pero ahora, gracias a la combinación de dos factores, es posible aplicar sus métodos y obtener beneficios. Estos factores son la recolección masiva de datos y el control sobre los diferentes estados de un proceso. Además, recientemente se han desarrollado herramientas que permiten trabajar con grandes cantidades de datos de manera rápida y profesional, como ProM, Disco y Celonis. Aunque estas herramientas utilizan algoritmos y métodos de gestión de procesos para resolver problemas recurrentes, las técnicas de minería de procesos también pueden aplicarse de manera más básica con lenguajes de programación o incluso con lápiz y papel, facilitando el análisis de datos y la generación de información.

En Ecuador, Alvarado Llano y Changoluisa Pachacama (2019), en su investigación “Análisis de la ciberseguridad a la infraestructura tecnológica de la universidad técnica de Cotopaxi”, definen la ciberseguridad, también conocida como seguridad informática, como la protección de la infraestructura computacional. Esto implica identificar los activos informáticos, sus debilidades y amenazas, así como la probabilidad de que ocurran y su impacto, con el fin

de determinar los controles adecuados para aceptar, reducir, transferir o evitar los riesgos de posibles ataques.

Capítulo II

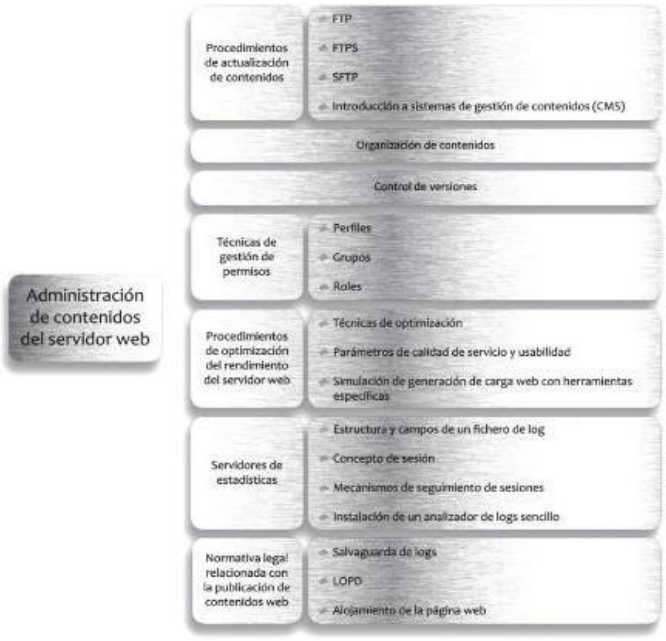
Marco Teórico

El servicio de Internet

Internet comenzó en la década de 1960 cuando Estados Unidos buscaba una manera de mantener las comunicaciones esenciales del país en caso de una guerra nuclear. Crearon una plataforma cuyas características fundamentales aún se mantienen en la red actual. Al mismo tiempo, esta tecnología se desarrollaba para otras aplicaciones, como el envío de correos electrónicos (Véase Figura 1). Ya en los años setenta, estas redes de computadoras comenzaron a expandirse (Peña Valenzuela, 2015).

Figura 1

Administración de Contenidos para sitios Web



Nota. Tomada del libro Manual. Administración y auditoría de los servicios Web (UF1272). Certificados de profesionalidad. Administración e servicios de Internet (IFCT0509) pag,14

“El creciente uso de Internet por parte de los usuarios ha hecho que las aplicaciones de gestión de contenido se vuelvan indispensables para los administradores de sitios web.”. (Carvajal Palomares, 2016)

Responsabilidad de los proveedores de internet

Según Peña Valenzuela (2013), aunque Internet no ha abandonado sus objetivos originales, ha evolucionado hasta convertirse en un universo paralelo de convivencia virtual. En este espacio, se establecen relaciones jurídicas y comerciales que pueden ser incluso más complejas que las del mundo físico. Con más de 2.000 millones de personas conectadas, conceptos jurídicos como la responsabilidad, el daño, la propiedad y la distinción entre lo público y lo privado deben ser reconsiderados al ritmo de la evolución e interacción en la red. pág. 56)

En el mundo moderno, donde las relaciones humanas se desarrollan a través de la tecnología y los vínculos jurídicos se concretan mediante ella, es crucial establecer la responsabilidad y definir cómo se reconocerán los diferentes actores que forman parte del universo tecnológico. (Manterola & Sondergaard, 2021).

Los usuarios

El último sujeto de internet es el usuario, destinatario principal del entramado de relaciones que suceden en la red. Los usuarios en principio son todos los destinatarios finales de toda la actividad que se produce en la red (Véase Figura 2). Esta idea tiene cabida en la definición que los señala como aquellos “que se benefician con los resultados de un proceso determinado” es decir como aquellos que reciben los resultados de todos los procesos que se producen entre los diferentes sujetos que participan en la internet. (Rengifo García, 2015)

Figura 2

Usuarios

Nota. Tomada de Google. https://www.google.com.ec/books/edition/Ciberseguridad/ZqHDDwAAQBAJ?hl=es&gbpv=1&dq=ataques+ciberneticos&printsec=frontcover.

La ciberseguridad

Hay que tener en cuenta que, las amenazas y riesgos a la ciberseguridad emanan de actores internacionales como el Estado, organizaciones e individuos quienes obtuvieran que las ciberarmas y ciberataques de larga trascendencia y bajo costo se multipliquen y vuelvan más sofisticado, ocasionando incluso el deceso de personas con medios digitales. Esto enlaza que la primera barrera de defensa es el usuario final de los sistemas informáticos, y por ello debe ser educado y concientizado sobre la importancia de la ciberseguridad en su existencia. Por ende, las medidas que se pueden implementar para garantizar la ciberseguridad nacional e internacional requieren de una visión integral que permita a los estados, la sociedad civil y las empresas asumir responsabilidades compartidas. (Arreola García, Ciberseguridad ¿Por qué es importante para todos?, 2019)

La protección de la información es una ocupación critica para todas las empresas, industrias y sociedades modernas. Proteger la información ha sido una primacía desde que las personas han necesitado conservar la información de una forma segura y privada. La ciberseguridad es un ejido cada vez más extenso y tornadizo, y es crucial que los conceptos

centrales que enmarcan y definen este campo sean entendidos por los profesionales que estén interesados e involucrados en las implicaciones de seguridad de las tecnologías de la información (TI). (Ortega Candel, 2021)

La ciberseguridad es la destreza de acogerlas computadoras, los servidores, los terminales móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. Así mismo, se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se utiliza en desiguales contextos, a partir los negocios hasta la informática móvil, y puede dividirse en algunas categorías frecuentes.

La ciberseguridad se apoya en varias disciplinas para ser efectiva, y una de las más importantes es el cifrado. Este mecanismo permite proteger la información transmitida a través de los navegadores mediante certificados digitales o protocolos SSL/TLS. Además, también permite el cifrado de archivos específicos. Afortunadamente, la evolución en este campo no se detiene y continúa avanzando para ofrecer la protección adecuada en el espacio cibernético. Esta disciplina es tan extensa que algunos se han atrevido a plantear fases que esta cumple, como prevención y localización. (Zorrilla Mateo, 2020)

Importancia de la ciberseguridad

Según Arreola García (2019), en el siglo XXI, la dependencia de los sistemas computarizados por parte del gobierno, las fuerzas armadas y las empresas privadas ha crecido exponencialmente. Sin embargo, esta dependencia también ha revelado las debilidades inherentes de estos sistemas digitales, poniendo en riesgo la seguridad de estados, organizaciones e individuos. Además, la creciente inmersión de la sociedad en el ciberespacio, debido a su fácil accesibilidad, ha hecho que las intrusiones clandestinas en este ámbito virtual sean cada vez más comunes, poderosas y preocupantes. pág. 3).

Tipos de ciberseguridad

Los requisitos de seguridad cibernética pueden definirse en función de los tipos de ataques que se observan con el tiempo. La seguridad de aplicaciones se refiere a proteger el

código dentro de las aplicaciones contra pérdidas o robos. La seguridad de red se encarga de establecer y proteger la infraestructura física. La seguridad cibernética, por su parte, protege los sistemas conectados en línea, mientras que la seguridad en la nube proporciona servicios de procesamiento de información a través de internet. En resumen, la seguridad en la nube puede definirse como los procedimientos y políticas adoptados para garantizar la seguridad cibernética. (Bakht, 2020)

Seguridad informática

Es común que se confundan dos términos: seguridad informática y seguridad de la información. Aunque parecen similares, tienen diferencias importantes. La seguridad informática se centra en proteger los sistemas informáticos. Según varios expertos, la informática es la ciencia que estudia los procesos, técnicas y métodos para procesar, almacenar y transmitir información.

Por otro lado, la seguridad de la información no se limita solo a los sistemas informáticos; se trata de proteger cualquier tipo de información, sin importar el medio en el que se encuentre. En resumen, esto significa que su alcance es mucho más amplio. La diferencia principal entre ambos conceptos radica en el ámbito que cada uno cubre dentro del mundo de la informática. (Romero Castro y otros, INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES, 2018)

Procesos operacionales

En las empresas de servicios, los clientes pueden involucrarse en el proceso de producción o prestación del servicio. Esto se debe a que una característica fundamental de los servicios es su “integridad o simultaneidad”. La interacción con el cliente durante la creación del servicio permite codificar los procesos operativos. En otras palabras, el grado de relación con el cliente es la variable que más influye en el diseño del proceso de prestación del servicio. (Martín Peña & Díaz Garrido, 2016)

Las TICs

Es el agregado transformado de herramientas y recursos tecnológicos consumidos para transmitir, almacenar, crear, compartir o intercambiar información. Estas herramientas y recursos tecnológicos contienen software, computadoras, internet (sitios web, blogs y correos electrónicos). Tecnologías de radio-difusión en directo (radio, televisión y difusión por internet). Tecnologías de radio-difusión grabada (podcasting, reproductores de audio y video y dispositivos de almacenamiento) y telefonía, fija o móvil y satelital (Echaiz & Flores, 2021) (Véase Figura 3)

Figura 3

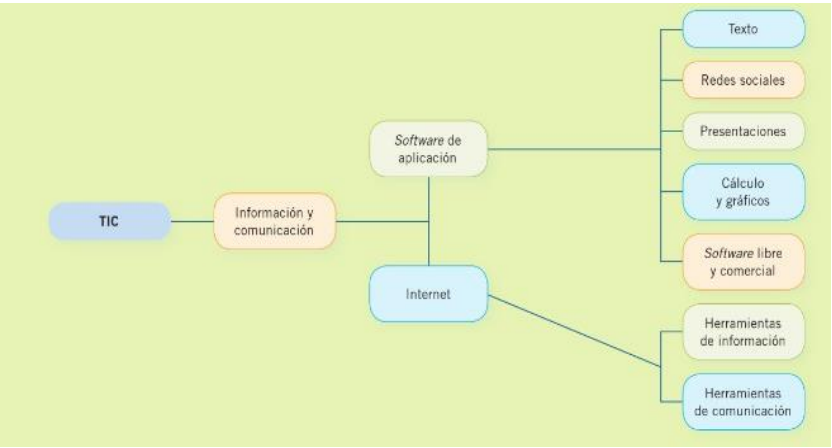
Tecnologías de la Información

Nota. Tomada de Google. https://www.google.com/search?client=firefox-bd&q=tic+imagenes&tbm=isch&sa=X&ved=2ahUKEwiY0aupvaCAAxU6SzABHVQID7kQ0pQJegQIChAB&bi w=1366&bih=635&dpr=1#imgrc=sE6n1oxYeIjiSM

Las tecnologías de la información y las comunicaciones (TIC) han sido y seguirán siendo dinámicas y progresivas, por hábitat, liderando la incidencia perpetua de nuevas tendencias tecnológicas y los negocios. Los adelantos en recursos de computación, sistemas de software y redes de comunicaciones incorporados a la continua miniaturización de los componentes hardware (sensores y dispositivos) han hecho posible un ecosistema de internet de las cosas inteligente y desplegado a lo largo de toda la superficie geográfica global. (Joyanes, Internet de las cosas, 2021) (Véase Figura 4)

Figura 4

Las TIC



Nota. Tomada de Google. https://www.google.com.ec/books/edition/Tecnolog%C3%ADas_de_la_Informaci%C3%B3n/6M1UCwAAQBAJ?hl=es&gbpv=1&dq=tecnolog%C3%ADa+de+la+informatica&printsec=frontcover

Estándar ISO 27000

"Las normas ISO 27000 se empieza a crear en 2005, no obstante existen normas similares de seguridad de la información bastante anteriores, como la BS 7799 de 1995 y la ISO 17799 de 2000". (Giménez Albacete, 2015)

Las normas ISO 27000 de la familia ISO/IEC-27000 conforman un conjunto de estándares orientados a las buenas prácticas, seguridad de la información y mitigación del

riesgo, relacionadas con la implementación, gestión y mantenimiento de un SGSI o sistema de gestión de la información y que también sigue la filosofía de mejora continua, conocida como ciclo Deming o PDCA, (Plan-Do-Check-Act), que es la abreviatura de las fases de este ciclo que son planificar, hacer, verificar y actuar. (Menéndez Arantes, 2022)

La serie de normas ISO/IEC-27000, desarrollada por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), es un conjunto de estándares reconocidos globalmente. Estas normas, respaldadas por numerosos países, aseguran una amplia difusión, implementación y aceptación en todo el mundo.

La serie 27000 se centra en establecer buenas prácticas para la implementación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI), conocido en inglés como Information Security Management System (ISMS). Estas guías buscan promover las mejores prácticas en la gestión de la seguridad de la información, con un fuerte enfoque en la mejora continua y la mitigación de riesgos.

Normas ISO 27001

Las normas ISO 27001 se han convertido en un estándar de referencia en la seguridad de los sistemas de información, especialmente en la implementación de un sistema de gestión de la seguridad de la información (ISO 27005). Se puede considerar como una adaptación de la normativa de calidad ISO 9001 al ámbito de la seguridad informática. Para mantenerse al día con las tecnologías emergentes, el conjunto de normas ISO 27001 ha experimentado una expansión significativa en los últimos años. (Carpentier, 2016)

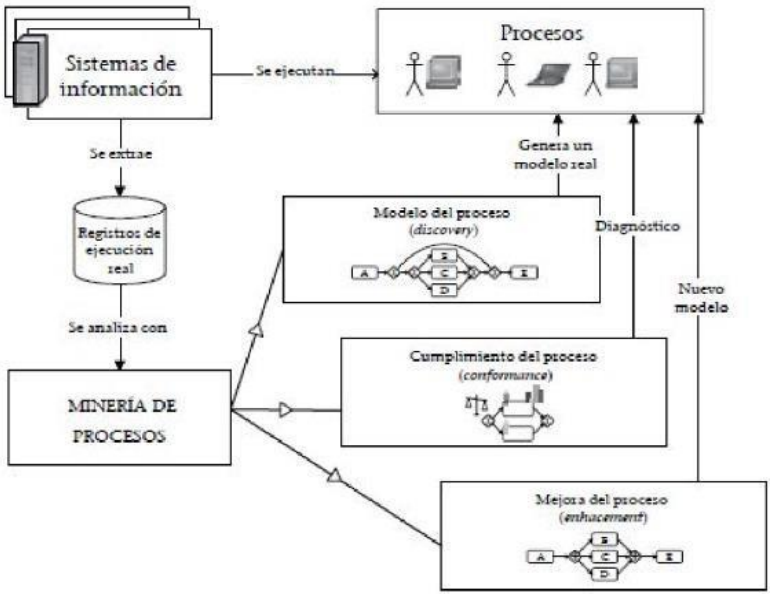
La asociación española de normalización y certificación (AENOR,2017) señala que la norma ISO 27001 detalla los requisitos de un Sistema de Gestión de la Seguridad de la Información (SGSI). Esta suministra un marco frecuente para la preparación de las normas de seguridad en cualquier organización, estableciendo un método de gestión confiable para la seguridad. (Hernández Bejarano, 2020)

Minería de procesos

La minería de procesos es una técnica diseñada para descubrir, monitorear y mejorar los procesos comerciales reales. Esto se logra extrayendo información valiosa de los registros de eventos de los sistemas de información. Por otro lado, las redes definidas por software buscan simplificar la complejidad de las redes tradicionales. Lo hacen automatizando las funciones de red, acelerando la ejecución de aplicaciones y servicios, y facilitando la implementación y gestión de los recursos de la red. (Véase Figura 5)

Figura 5

Esquema de una Minería de Procesos



Nota. Tomada de Google. https://www.google.com.ec/books/edition/Miner%C3%ADa_de_procesos/5J4xDwAAQBAJ?hl=es&gbpv=1&dq=que+es+una+mineria+de+procesos&printsec=frontcover

"La minería de procesos es una disciplina cuyo objetivo es descubrir, monitorear y mejorar procesos mediante la extracción de conocimientos de los registros de eventos de los sistemas de información". (Aguirre Mayorga, 2016)

Tipos de minería de Procesos

El primer tipo de minería de procesos es el descubrimiento. Esta técnica toma un registro de eventos y genera un modelo sin utilizar información previa. El descubrimiento de procesos es la técnica de minería de procesos más destacada. Para muchas organizaciones, es sorprendente ver cómo las técnicas actuales pueden realmente descubrir los procesos reales basándose únicamente en las muestras de ejecución de los registros de eventos.

El segundo tipo de minería de procesos es la conformidad. En este caso, se compara un modelo de proceso existente con un registro de eventos del mismo proceso. La verificación de conformidad puede ser útil para comprobar si la realidad, tal como está registrada en el registro de eventos, coincide con el modelo y viceversa.

El tercer tipo de minería de procesos es la mejora. Aquí, la idea es extender o mejorar un modelo de proceso existente utilizando la información sobre el proceso real almacenada en algún registro de eventos. (Hitpass, 2017) (Véase Figura 6)

Figura 6

Tipos de Minería de Procesos

Nota. https://www.google.com.ec/books/edition/BPM_Business_Process_Management/Dm4-MGAy5vMC?hl=es&gbpv=1&dq=tipos+de+miner%C3%ADa+de+procesos&pg=PA219&printsec=frontcover.

Herramientas de minería de procesos

En cualquier sistema de información, lo más crucial no es el hardware ni el software, ya que estos pueden ser reemplazados en cualquier momento, a diferencia de los datos. La cantidad de información sigue creciendo y es necesario acceder a los datos lo más rápido posible. Por lo tanto, los procesos para su gestión adecuada y eficiente, considerando los costos asociados, son uno de los objetivos principales en cualquier sistema de información. (POSTIGO PALACIOS, 2020)

ProM

“Esta herramienta almacena la información de acuerdo a un modelo que refleja la información de los usuarios, los proyectos y los eventos generados por usuario, permitiendo realizar un análisis básico de los datos”. (Piattini Velthuis y otros, 2019)

Política de seguridad

La política de seguridad tiene como objetivo principal definir la protección de los sistemas de información de la empresa. Establece una base para desarrollar estrategias, directrices, procedimientos, códigos de conducta y normas tanto organizativas como técnicas. Esta política asegura que la implementación de medidas de seguridad sea adecuada a los usos, económicamente viable y conforme a la legislación vigente. Debe estar documentada formalmente en la empresa y puede incluir un resumen de las prácticas que guían la gestión de la seguridad.

De acuerdo con Romero Castro, Figueroa Morán, Vera Navarrete, Álava Cruzatty, & Parrales Anzúles, 2018La mayor parte de los ataques informáticos se consiguen evitar o por lo menos reducir el impacto, si se hiciera manipulando los mecanismos preventivos, falta de sistemas y otros problemas podrían hallar, evitarse y resolverse gracias a un buen trabajo durante esta etapa. La barrera más enérgica a la que se afronta una empresa al querer aplicar los mecanismos preventivos es la aceptación y el compromiso de todos los involucrados, hacer

entender que no es una carga, es parte de los procesos y lo que se debe hacer bien en la organización pág. 124.

Capítulo III

Metodología de la investigación

Descripción de la metodología

Para la presente investigación, se desplegaron métodos y técnicas de investigación de alta efectividad, con el propósito de obtener información relevante que aporte significativamente el desarrollo investigativo, a través de la recopilación de los datos pertinentes y de sumo interés en los diferentes eventos planteados a través de los objetivos de esta línea investigativa, en las instalaciones la empresa de servicio de internet en la ciudad de Milagro periodo 2022.

Método Deductivo

Este método resultó significativo para la investigación, ya que a través del mismo se logró obtener toda la información que sirvió de aporte de acuerdo a la investigación teórica, basada en libros, revistas y ensayos de investigadores cuyos aportes teóricos son reconocidos, comprobados y veraces, guiando teóricamente esta investigación.

> “Es más beneficioso de las ciencias formales (como la matemática y la lógica), convive en ir de lo corriente a lo personal, mediante el uso de argumentos y/o consecuencia. En el que se utiliza la lógica para llegar a terminaciones, a partir de determinadas premisas”. (Zarzar Charur, 2015)

Método Inductivo

A través de la aplicación de este método la investigación a través de la información recopilada, que permitió llegar a las conclusiones del caso, basándose en los principios de observación y análisis de los datos recopilados para la misma, y el soporte investigativo a lo largo del presente trabajo.

“Que es más conveniente de las ciencias sociales, consiste en ir de lo personala lo general. A partir de la reflexión de los hechos, se crean leyes mediante la generalización del comportamiento observado”. (Zarzar Charur, 2015)

Método Analítico

Mediante este método, se puede analizar de manera concisa los hechos estudiados a partir de la recopilación de datos y teorías, que fundamentan de forma crítica y objetiva la línea investigativa, a través de los hechos y objetivos planteados a partir de la detección del problema.

Población y muestra

La población tomada para esta investigación es de carácter finita, por lo que no es necesaria la aplicación de una fórmula para obtener una muestra, simplemente los instrumentos de investigación fueron orientados y aplicados a su población total de 10 empleados de la empresa de servicio de internet dentro de la ciudad de milagro y una pequeña muestra de 10 clientes, tomado de forma aleatoria para la aplicación de la entrevista y las encuestas respectivas.

Técnicas de Investigación

En el perímetro de la investigación y durante los últimos años se ha mostrado un "enfrentamiento" entre teorías y prácticas que protegen, por un lado, un camino atributivo, y por el otro, un rumbo cuantitativo. Las discrepancias se han radicalizado y se han tomado posiciones irreconciliables. Cada uno afirma en ser el enfoque adecuado y oportuno para la investigación. Defienden sus sustentos teóricos, sus técnicas y procedimientos como los más adecuados. (Campos Arenas, 2021).

La presente investigación posee características cuali-cuantitativas, debido a su composición investigativa. Estas cualidades hacen de esta investigación basada en datos que permite analizar sus cualidades a través de las técnicas de investigación, así como técnicas que analiza datos y aportan características cuantitativas a la misma.

Esta investigación posee características cuali-cuantitativas, que, a partir de los hechos estudiados, se ha podido verificar los tintes investigativos a través de su desarrollo y análisis de la información recopilada de las diferentes fuentes e instrumentos de investigación, para

proceder a analizar los datos que permitan cuantificar las variables pertinentes a esta investigación.

Cualitativa

Así, esta investigación cualitativa sobrelleva, en todo el proceso de su progreso, el desarrollo por parte del científico de un conjunto de prácticas afines con las decisiones que las preceden y que están encaminadas a resolver, por un lado, qué y con qué método investigar, como consentir a los datos y como interpretarlos y, por el otro, como representar los resultados alcanzados. (Denzin & Lincoln, 2015)

Cuantitativa

“Esta investigación tiene que ver con la medición, revisión, descripción, experimentación, verificación y explicación del fenómeno objeto de estudio”. (Maldonado Pinto, 2018)

Instrumentos de Investigación

Encuestas

Se procedió a la aplicación de las encuestas, aplicadas de forma aleatoria a una muestra reducida de diez clientes, en las cuales se plasmaron preguntas cerradas, para conocer la calidad de atención que reciben en el servicio.

Cuestionarios

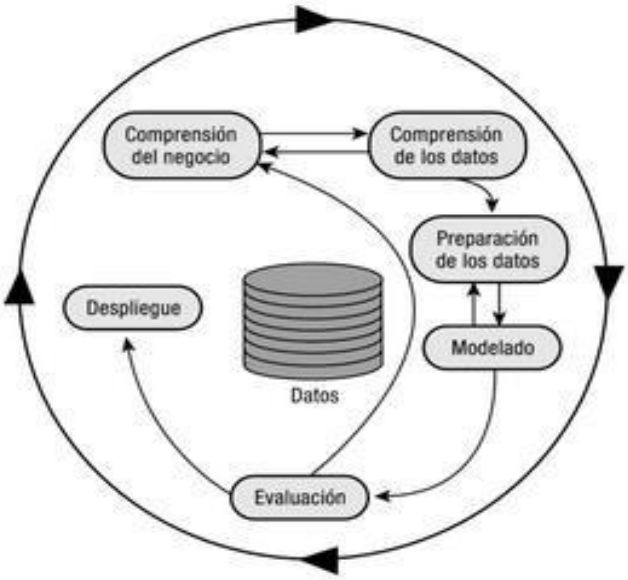
La aplicación del cuestionario está dirigido a todos los colaboradores de la empresa, en donde su resultado dio a conocer el riesgo que infiere la ciberseguridad y los procesos operativos dentro de la empresa. Así como también se procedió a la evaluación del cuestionario de aplicabilidad de las ISO27001 dentro de la empresa dirigida a todo el personal.

Lifecycle model for Process Mining

Esta metodología plantea el ciclo de vida de un proceso, que consta de seis etapas que comienzan con una buena comprensión y conocimiento del negocio y la necesidad del proyecto, y concluye con el despliegue de la solución que cumple y la necesidad específica del negocio, estas etapas son secuenciales por naturaleza, pero con un gran enfoque en la realimentación o backtrancking. (Joyanes, Sistemas de Información en la empresa, 2015) (Véase Figura 7)

Figura 7

Fases de la metodología

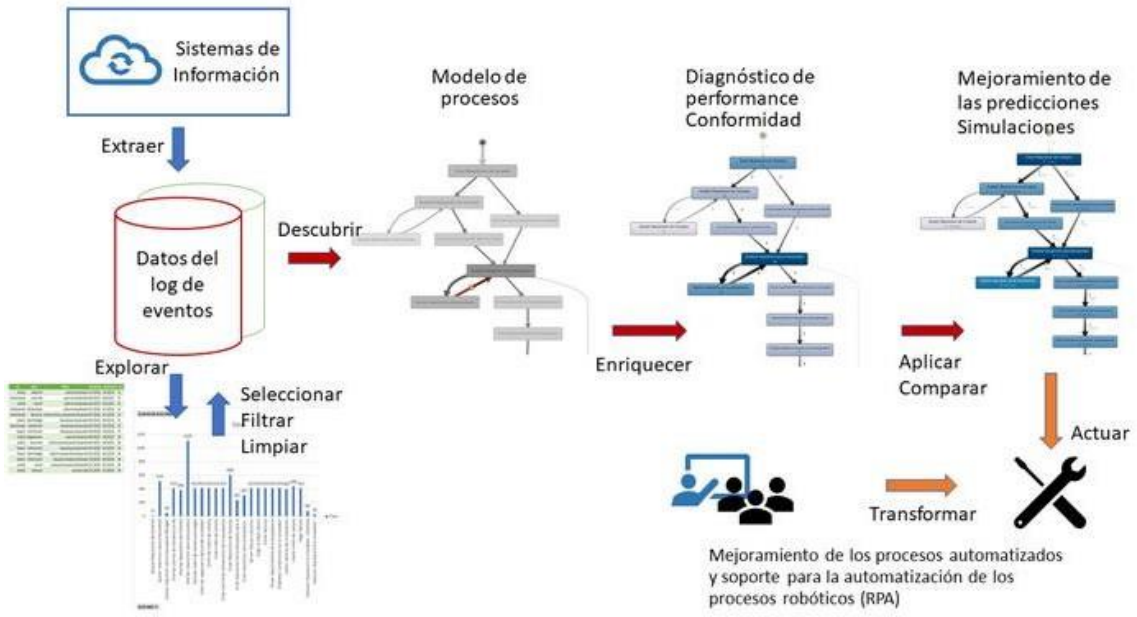


Nota. Tomado del libro (Joyanes, Sistemas de Información en la empresa, 2015, pág. 301)

La seguridad perpetuamente indaga la gestión de riesgo, esto quiere decir que se tenga constantemente una forma de evadirlo o prevenirlo y que se pueda realizar ciertas acciones para evitar esas situaciones de la mejor forma. (Romero Castro y otros, INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES, 2018) (Véase Figura 8)

Figura 8

Práctica en pleno crecimiento

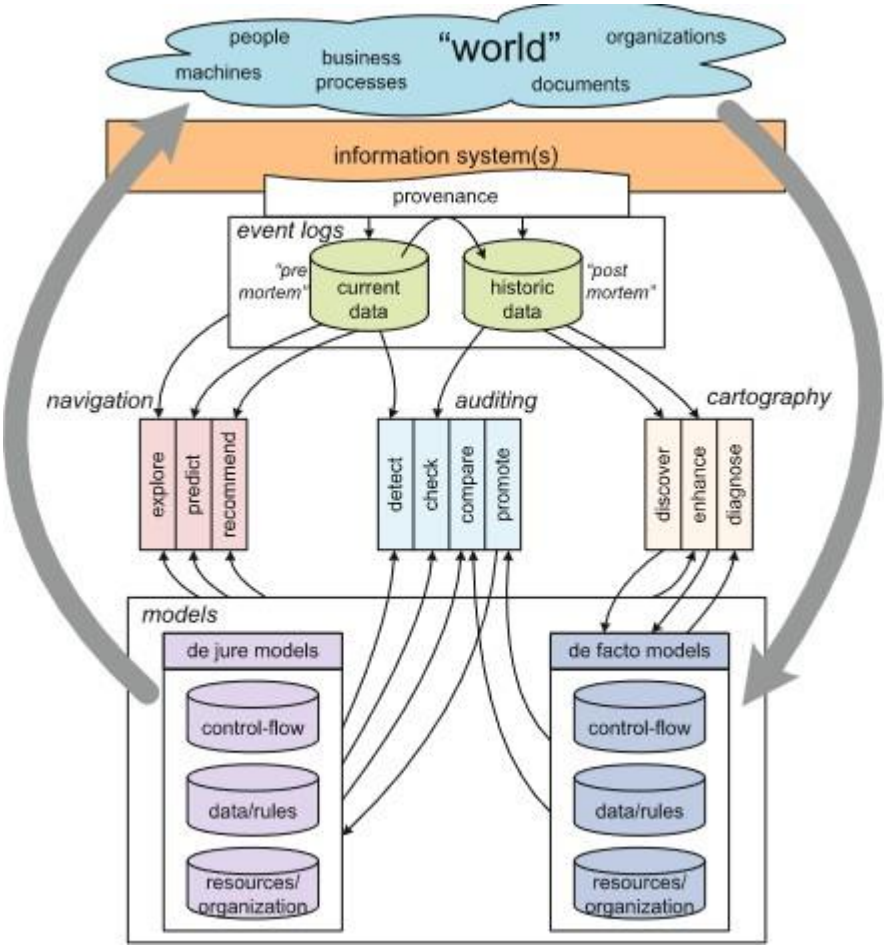


Nota. Tomado de (Romero Castro y otros, INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES, 2018)

Se puede describir esta metodología mediante el ciclo de vida, que optimiza y protege los procesos y la información que estos contienen, mediante la utilización de datos de diferentes sucesos o eventos, que sirven de contingencia en la protección de la seguridad informática. (Véase Figura 9)

Figura 9

Proceso de la información a través de la Process Mining

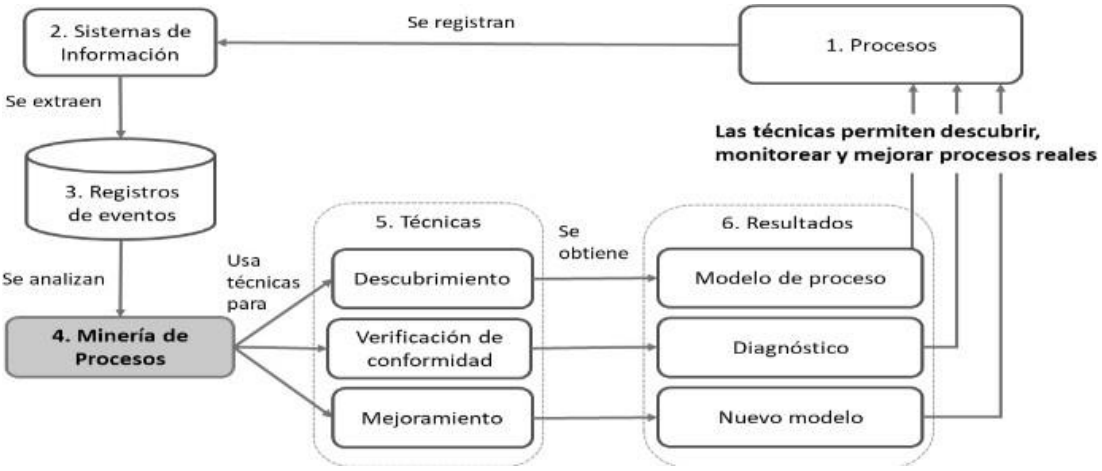


Nota. Tomado del libro Process Mining de (Van der Aalst, 1998, pág. 283)

Se necesita ubicar los datos a ser procesados, de acuerdo a la base estructural de datos lógicos de la empresa, con el fin de unir estos datos de manera operativa y cuya secuencia sea de aporte significativo al objetivo planteado, de medir, observar, monitorear y mejorar los procesos reales ya establecidos. Esto se logra en conjunto con la extracción de los conocimientos del logaritmo de eventos. (Véase Figura 10)

Figura 10

Modelo del proceso de acuerdo a la extracción de la información de una minería de procesos



Nota. Adaptación del libro original de (Van der Aalst, Wil M, 2011)

Se analiza el comportamiento almacenado en el log de eventos, para saber si de esta manera es factible o no la ejecución del proceso y así poder aprobar los procesos operacionales a través de la aplicación del ciclo de vida del producto o Lifecycling model.

Planificación y Justificación. Basados, fundamentados y orientados a la seguridad de la información, a través de la minería de procesos integrados en los datos operativos de la empresa, se procedió a identificar la información reflejada en los datos necesarios para la extracción de la información.

Extracción de datos. Una vez establecido el proyecto e identificado el objetivo central del mismo, se procede a extraer la información de los eventos cuantificados y reflejados en los datos extraídos del sistema.

Creación del modelo de flujo y control de eventos. En cuanto al flujo del control, este es el eje y soporte principal del modelado, que analiza los procesos operacionales, aprovechando las ventajas que este método y la tecnología ofrecen a favor.

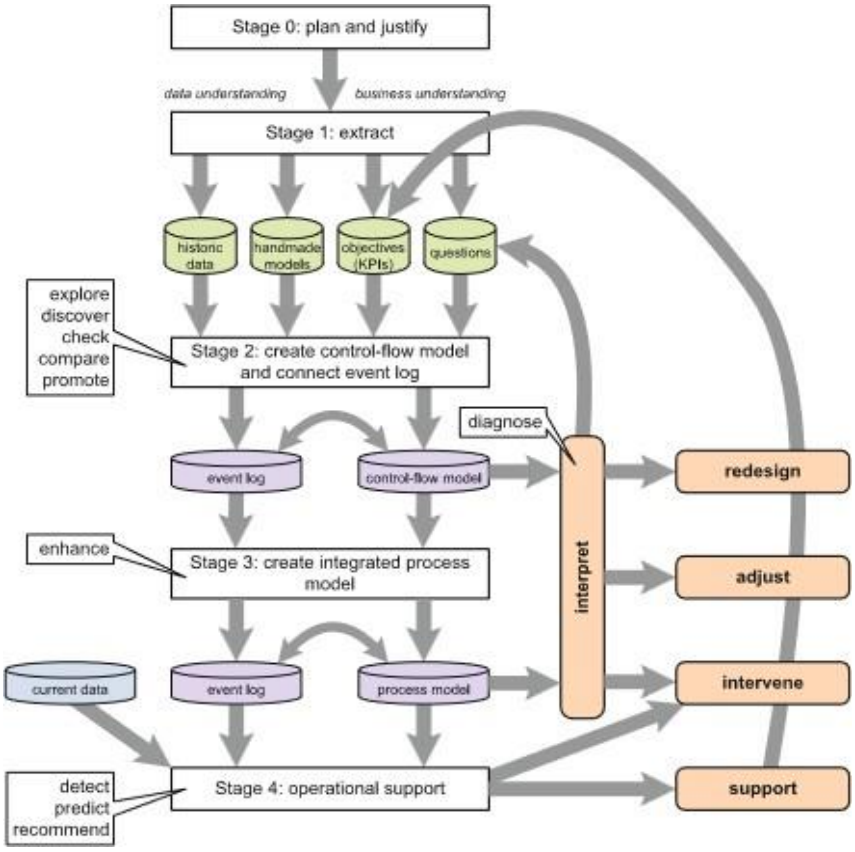
Crear el modelo de proceso integrado. En esta etapa ya se visualiza si la aplicación de este modelo ha logrado mejorar o alcanzar un avance en cuanto al modelo original de la empresa y lo que pretende a través de la utilización del mismo.

Soporte Operativo. A través de este modelo, se detecta, predice y da paso a recomendar de manera útil y acertada el uso y tiempo del modelo a seguir dentro de la empresa y los beneficios que este trae referente al modelo ya establecido.

Aplicación. A través de la aplicación ya culminada, se obtienen los parámetros a implementar, en cuanto a lo deseado a través de la aplicación de esta metodología, orientada a los procesos y seguridad de ejecución de los mismos y la información que en ellos fluctúa. (Véase Figura 11)

Figura 11

Aplicación de la metodología



Nota. Tomada del Libro Process Mining de (Van der Aalst, 1998, pág. 284)

Capítulo IV

Resultados

En este capítulo se desarrollará y evaluará el resultado de las técnicas e instrumentos de investigación, utilizados para corroborar las variables inmersas dentro de los objetivos planteados para la realización de la presente. Así como la demostración de la propuesta implementada como estrategia dentro de la solución del problema central investigativo.

Encuestas

¿Qué opinión tiene sobre nuestro servicio de internet?

De acuerdo a la opinión que los clientes tienen acerca de nuestro servicio de internet, el 47% de los encuestados estuvieron de acuerdo que el servicio que se ofrece es bueno, mientras que en otro escenario el 20% indicó que era un mal servicio el que reciben. (Véase Tabla 1 y Figura 12)

Tabla 1

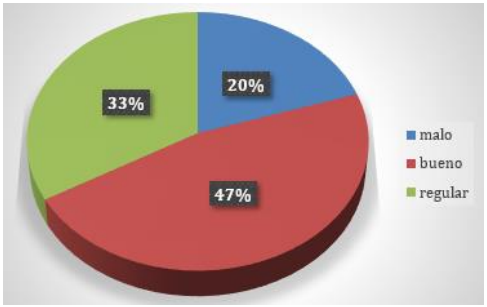
Opinión del cliente.

Alternativas	Valor Absoluto	Valor Relativo
Malo	3	20%
Bueno	7	47%
Regular	5	33%
Total	15	100%

Nota. Tomado de encuesta (2025)

Figura 12

Opinión del cliente



Nota. Tomado de encuesta (2025)

2. En una escala del 0 al 5, seleccione, donde 5 representa la calificación más alta y 1 la más baja ¿Cuál es su nivel de satisfacción del servicio?

Con respecto a esta pregunta el 60% estuvo de acuerdo en que están satisfechos con el servicio, mientras que el 13% indico no sentirse satisfecho con el mismo. (Véase Tabla 2 y Figura 13)

Tabla 2

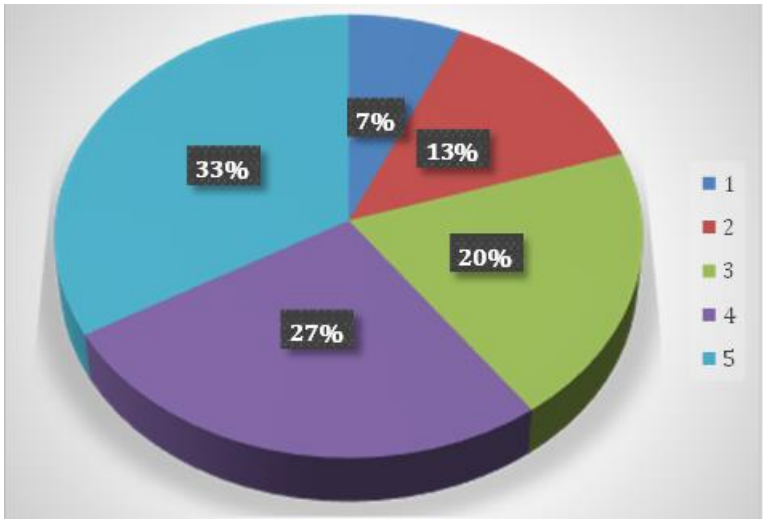
Nivel de satisfacción del cliente.

Alternativas	Valor Absoluto	Valor Relativo
1	0	0%
2	0	0%
3	2	13%
4	9	60%
5	4	27%
Total	**15**	**100%**

Nota. Tomado de encuesta (2025)

Figura 13

Nivel de satisfacción del cliente



Nota. Tomado de encuesta (2025)

3 ¿Cumple con sus expectativas nuestro servicio?

El 47% de los clientes encuestados indicaron que, si cumple con sus expectativas esperadas, frente a 47% que indicó lo contrario. (Véase Tabla 3 y Figura 14)

Tabla 3

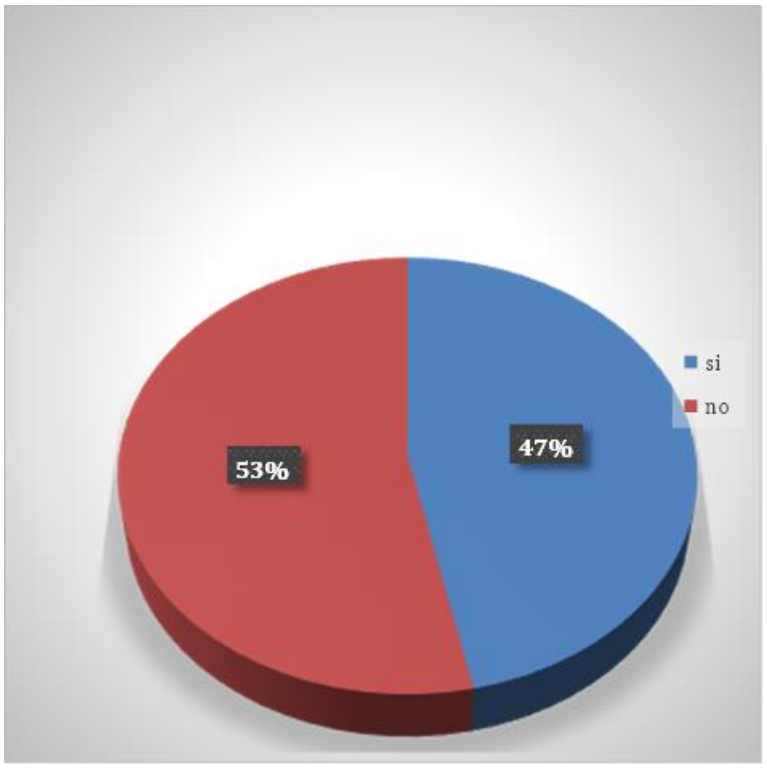
Expectativas acerca del servicio.

Alternativas	Valor Absoluto	Valor Relativo
si	7	47%
no	8	53%
Total	**15**	**100%**

Nota. Tomado de encuesta (2025)

Figura 14

Expectativas acerca del servicio



Nota. Tomado de encuesta (2025)

4. ¿Le parece módico el precio que paga por nuestro servicio?

Con respecto a esta pregunta el 60% indicó que el precio por el que pagan el servicio es módico, mientras que un 40% indico lo contrario. (Véase Tabla 4 y Figura 15)

Tabla 4

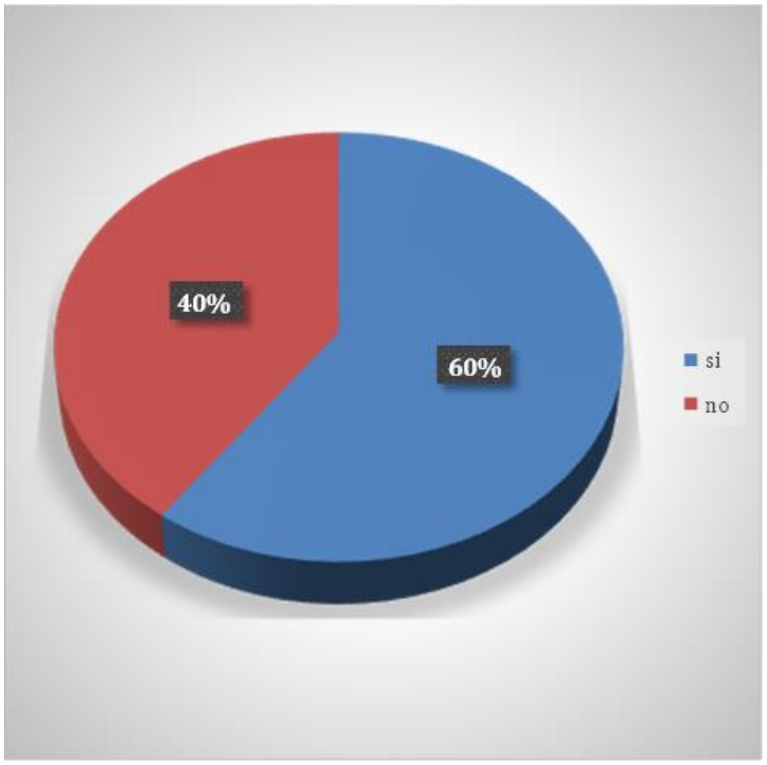
Opinión sobre el precio del servicio.

Alternativas	Valor Absoluto	Valor Relativo
si	7	47%
no	8	53%
Total	**15**	**100%**

Nota. Tomado de encuesta (2025)

Figura 15

Opinión sobre el precio del servicio



Nota. Tomado de encuesta (2025)

5. ¿Nuestro servicio ha logrado satisfacer necesidades?

El 67% de los encuestados indicaron sentirse satisfechos con las necesidades cubiertas a través del servicio de internet, mientras que el 33% restante mostraron insatisfacción en los resultados de esta interrogante. (Véase Tabla 5 y Figura 16)

Tabla 5

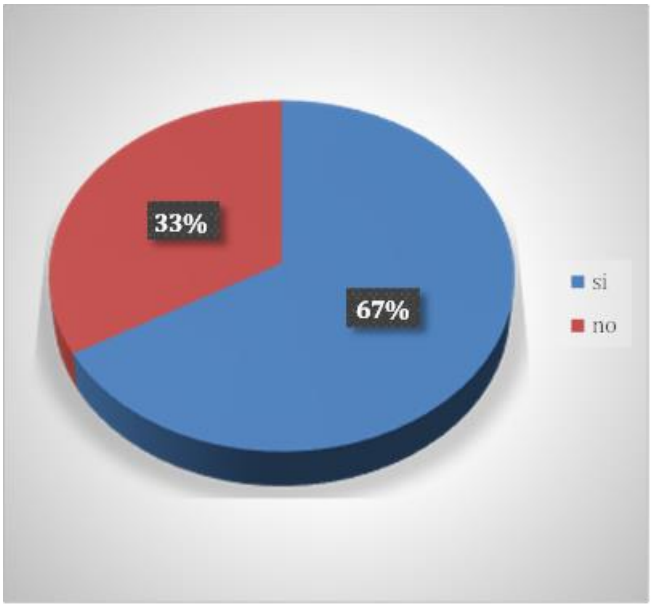
Satisfacción de necesidades a través del servicio de internet.

Alternativas	Valor Absoluto	Valor Relativo
sí	10	67%
no	5	33%
Total	**15**	**100%**

Nota. Tomado de encuesta (2025)

Figura 16

Satisfacción de necesidades a través del servicio de internet



Nota. Tomado de encuesta (2025)

6. ¿Ha tenido algún problema con respecto a la calidad del servicio?

El 67% de los encuestados indicaron no tener inconvenientes con el servicio de internet, mientras que el 33% restante indicaron que si han surgido inconvenientes. (Véase Tabla 6 y Figura 17)

Tabla 6

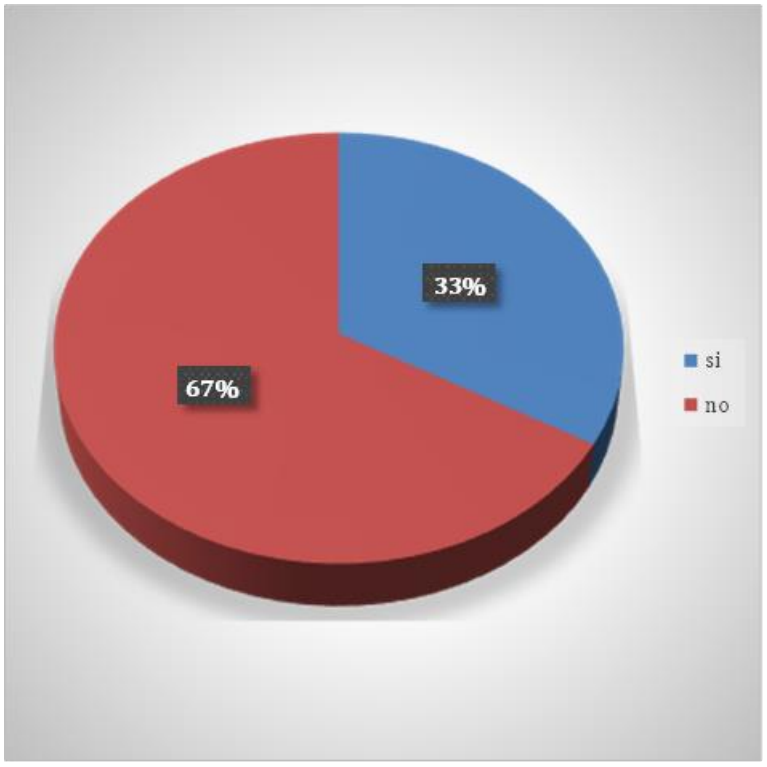
Inconvenientes en la calidad de servicio.

Alternativas	Valor Absoluto	Valor Relativo
si	5	33%
no	10	67%
Total	**15**	**100%**

Nota. Tomado de encuesta (2025)

Figura 17

Inconvenientes en la calidad de servicio



Nota. Tomado de encuesta (2025)

7. ¿Con que frecuencia utiliza el servicio?

El 100% de los encuestados indicaron utilizar el servicio de internet más de una vez por día, lo que lo convierte en indispensable. (Véase Tabla 7 y Figura 18)

Tabla 7

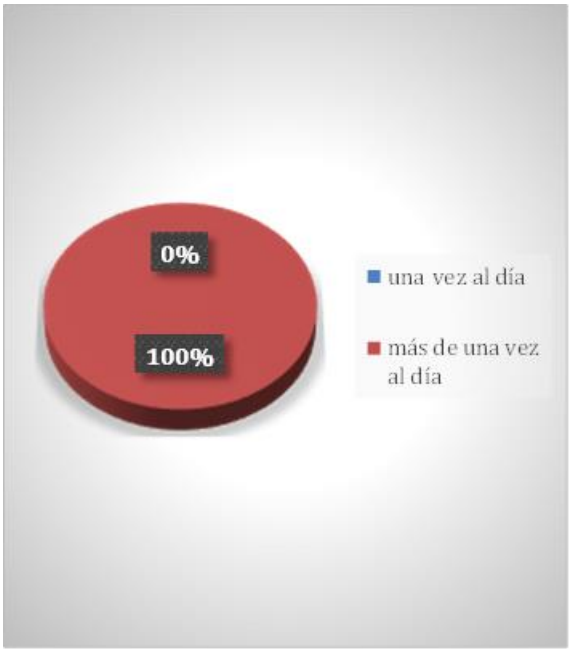
Frecuencia de utilización del servicio.

Alternativas	Valor Absoluto	Valor Relativo
una vez al día	0	0%
más de una vez al día	15	100%
Total	**15**	**100%**

Nota. Tomado de encuesta (2025)

Figura 18

Frecuencia de utilización del servicio



Nota. Tomado de encuesta (2025)

8. ¿Le preocupa la seguridad de la información digital que maneja a través de nuestro servicio?

El 60% de los encuestados indicaron sentir preocupaciones en la utilización del servicio. (Véase Tabla 8 y Figura 19)

Tabla 8

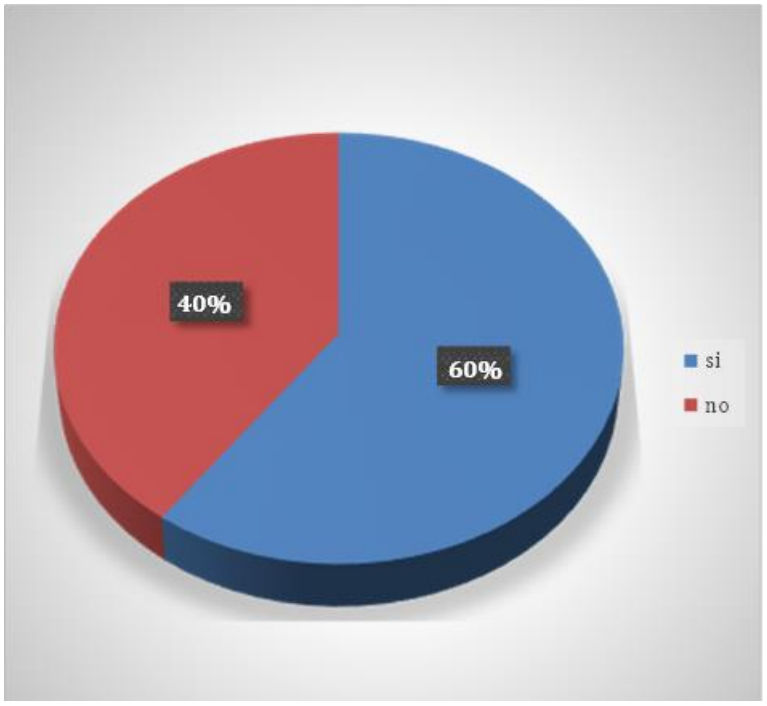
Preocupaciones de los clientes en cuanto al servicio de internet.

Alternativas	Valor Absoluto	Valor Relativo
si	9	60%
no	6	40%
Total	**15**	**100%**

Nota. Tomado de encuesta (2025)

Figura 19

Preocupaciones de los clientes en cuanto al servicio de internet



Nota. Tomado de encuesta (2025)

9. ¿Maneja información importante a través de sus plataformas digitales y demás dispositivos?

El 73% de los encuestados aseguraron manejar información importante a través del servicio que se ofrece. (Véase Tabla 9 y Figura 20)

Tabla 9

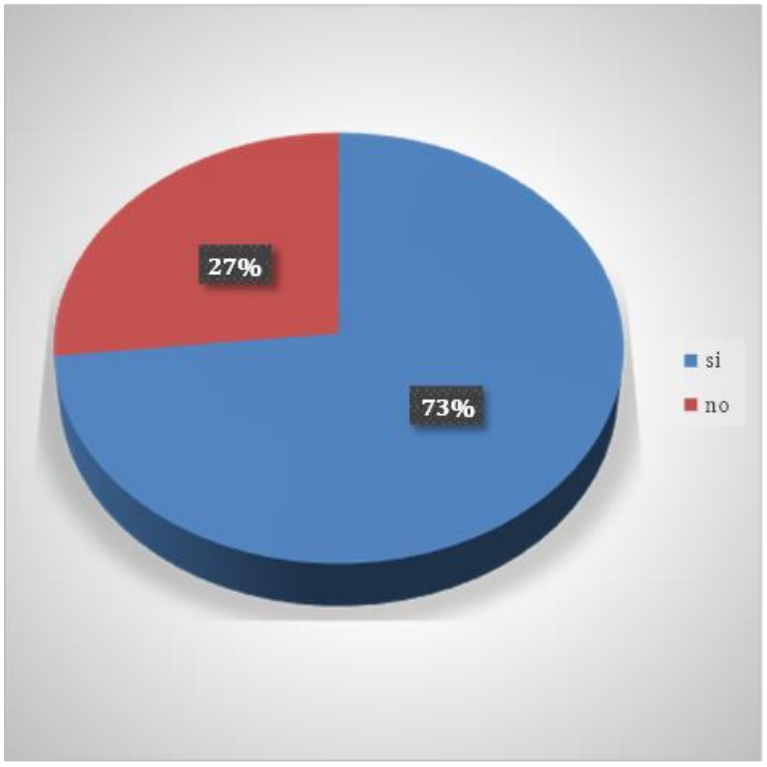
Manejo de información.

Alternativas	Valor Absoluto	Valor Relativo
si	11	73%
no	4	27%
Total	**15**	**100%**

Nota. Tomado de encuesta (2025)

Figura 20

Manejo de información



Nota. Tomado de encuesta (2025)

10. ¿Con cuánta frecuencia realiza compras a través de la web?

El 73% de los encuestados indicaron que siempre realizan compras a través de la web.

(Véase Tabla 10 y Figura 21)

Tabla 10

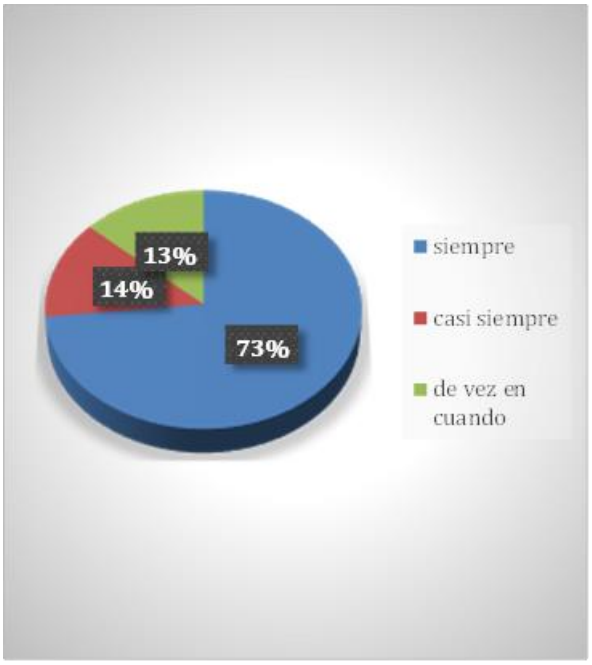
Frecuencia de compras por internet.

Alternativas	Valor Absoluto	Valor Relativo
siempre	11	73%
casi siempre	2	13%
de vez en cuando	2	13%
Total	**15**	**100%**

Nota. Tomado de encuesta (2025)

Figura 21

Frecuencia de compras por internet



Nota. Tomado de encuesta (2025)

11. ¿Considera importante que la empresa tenga un sistema que proteja la información y así evitar el ingreso de virus a través del servicio que utiliza?

El 80% de los usuarios consideran de gran relevancia la protección del servicio de internet contra el hurto de información relevante. (Véase Tabla 11 y Figura 22)

Tabla 11

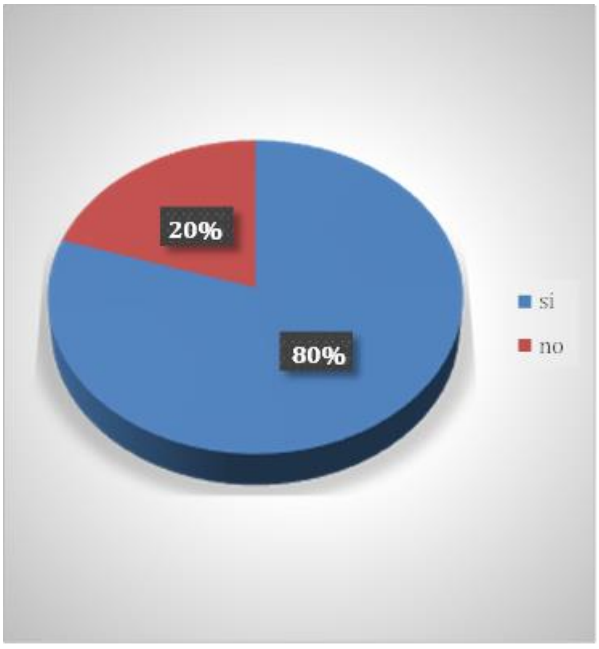
Sistema de protección de internet.

Alternativas	Valor Absoluto	Valor Relativo
si	12	80%
no	3	20%
Total	**15**	**100%**

Nota. Tomado de encuesta (2025)

Figura 22

Sistema de protección de internet



Nota. Tomado de encuesta (2025)

12. ¿Cambiaría de proveedor en caso de que su información y su red de distribución web se encuentren amenazados con respecto a la ciberseguridad de la misma?

El 100% coincidieron en cambiar de proveedor de internet en caso de que la información que manejan se vea vulnerada. (Véase Tabla 12 y Figura 23)

Tabla 12

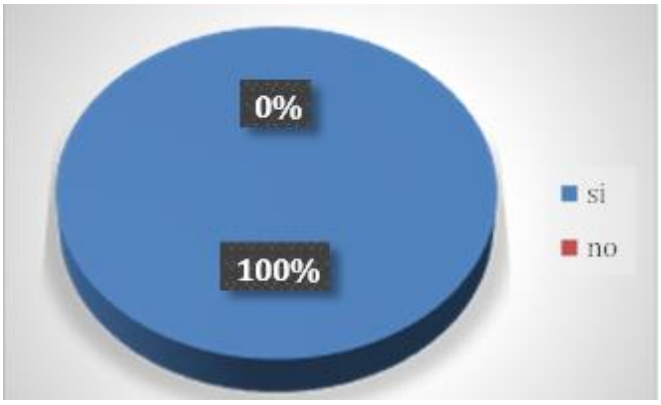
Información vulnerada.

Alternativas	Valor Absoluto	Valor Relativo
si	15	100%
no	0	0%
Total	**15**	**100%**

Nota. Tomado de encuesta (2025)

Figura 23

Información vulnerada



Nota. Tomado de encuesta (2025)

13. ¿Si pudiera mejorar algo de nuestro servicio que sería?

La mayoría de los encuestados coincidieron que lo que mejorarían en el servicio que se ofrece es la protección de la ciberseguridad y la calidad que ofrecen. (Véase Tabla 13)

Tabla 13

Mejoras en el servicio.

Alternativas	Valor Absoluto	Valor Relativo
la ciberseguridad	7	47%
la calidad del servicio	7	47%
nada	1	7%
Total	**15**	**100%**

Nota. Tomado de encuesta (2025)

14. ¿De acuerdo a su experiencia en cuanto a la utilización de nuestro servicio, ¿Lo recomendaría a sus amigos o familiares?

El 60% de los encuestados estuvieron de acuerdo en la recomendación del servicio de internet ofrecido. (Véase Tabla 14 y Figura 4)

Tabla 14

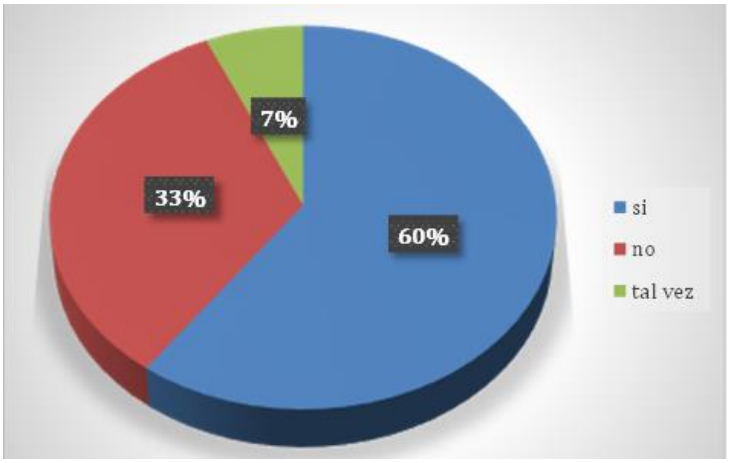
Recomendar el servicio.

Alternativas	Valor Absoluto	Valor Relativo
si	9	60%
no	5	33%
tal vez	1	7%
Total	**15**	**100%**

Nota. Tomado de encuesta (2025)

Figura 24

Recomendar el servicio



Nota. Tomado de encuesta (2025)

Cuestionario de análisis del control interno de la ciberseguridad

A través de la aplicación de este cuestionario, se obtuvo información oportuna y necesaria, para conocer el control que existe en la empresa de servicio en cuanto la protección de la seguridad de la información digital y de los sistemas operativos, cuya calificación total es sobre 10 cada ítem, evaluando los riesgos presentes y la manera en cómo son manejados los procesos y si existe el adecuado control. (Véase Tabla 15 y Tabla 16)

Tabla 15

Control interno de la ciberseguridad.

No.	Evaluación del riesgo de los procesos operacionales	Sí (10)	No (0)	Calificación /10
1	¿Existe una correcta ejecución y administración de los procesos operativos en cuanto a la ciberseguridad del mismo		X (0)	
2	¿Cuentan con un sistema operativo de seguridad que mitigue el fraude interno y externo?		X (0)	
3	¿Cuentan con una adecuada planificación cibernética que evite las fallas tecnológicas en cuanto al servicio?		x (0)	
4	¿Considera que brinda un servicio de buena calidad a sus consumidores?	X (0)		

5	¿Posee un plan o respaldo de contingencia en caso de fuga de información o tecnología?	X (0)	
TOTAL		**10**	**50**

Nota. Datos recopilados a través de la aplicación del cuestionario (2025)

Tabla 16

Control interno de la ciberseguridad.

CALIFICACIÓN TOTAL	**10**
PONDERACIÓN TOTAL	**50**

Nota. Datos recopilados a través de la aplicación del cuestionario (2025)

$$Nivel\ de\ confianza = \frac{Evaluación\ de\ riesgo\ alcanzado}{Evaluación\ de\ riesgo\ óptimo} * 100$$

$$Nivel\ de\ confianza = \frac{10}{50} * 100$$

$$Nivel\ de\ confianza = \ 20\%$$

$$Nivel\ de\ riesgo = \ 100\% - Nivel\ de\ confianza$$

$$Nivel\ de\ riesgo = \ 100\% - 20\%$$

$$Nivel\ de\ riesgo = \ 80\%$$

En el análisis de aplicación de este cuestionario, se evidenció un riesgo elevado del 80% en cuanto al incumplimiento de protección contra la ciberseguridad y un nivel bajo de confianza de utilización de la misma de un 20%, lo que conlleva a adoptar una medida que mitigue con dicho riesgo.

Cuestionario de evaluación del cumplimiento de las normas ISO 27001

100% de disponibilidad para el cumplimiento de un sistema de protección de ciberseguridad acogido a las normas ISO 27001. (Véase Tabla 17 y Tabla 18)

Tabla 17

Evaluación del cumplimiento ISO 27001.

COMPONENTES EVALUADOS	OBSERVACIÓN	CUMPLIMIENTO
Sistema de gestión de seguridad de la información	Es aplicable a los requisitos de las ISO 27001	SI
La empresa puede mantener y mejorar de manera continua el sistema de gestión de seguridad de acuerdo a los requisitos.	Acogido a la norma internacional ISO 27001	SI
Tratamiento de los riesgos en seguridad de la información	Declaración de aplicabilidad	Si
Objetivos de seguridad	Ser comunicados	SI
	Estar en constante actualización siempre y cuando sea apropiado	

Nota. Datos recopilados a través de la aplicación del cuestionario (2025)

$$= \frac{Cumplimiento}{Total, de\ componentes\ evaluados\ de\ acuerdo\ a\ las\ ISO\ 27001} * 100$$

$$= \frac{5}{5} * 100$$

Tabla 18

Nivel de confianza y aplicabilidad. Datos recopilados a través de la aplicación del cuestionario.

Aplicabilidad		
Bajo	**Moderado**	**Alto**
15% - 20%	51% - 75%	76% - 100%

Basados en la ciberseguridad orientados a la solución factible de la minería de datos aplicados bajo un modelo de gestión operacional, explicados en el capítulo III de la metodología de esta investigación, se evidencio un carecimiento de un modelo orientado y enfocado en las Normas ISO 27001.

Capítulo V

Propuesta

La minería de procesos proporciona un nuevo medio para mejorar los procesos en una variedad de aplicaciones y denominaciones. Hay dos impulsores principales para esta nueva tecnología. Por un lado, cada vez se registran más eventos, lo que proporciona información detallada sobre la historia de los procesos. A pesar de la omnipresencia de los datos de eventos, la mayoría de las organizaciones diagnostican problemas basándose en la ficción más que en los hechos. Por otro lado, los promotores del software Business Process Management (BPM) y Business Intelligence (BI) ha estado prometiendo milagros. Aunque las tecnologías BPM y BI recibieron mucha atención, no estuvieron a la altura de las expectativas planteadas por académicos, consultores y vendedores de software. (Van der Aalst, 1998)

La minería de procesos es una herramienta poderosa que ayuda a Modelar, Descubrir y mejorar los procesos de una organización, de acuerdo a los fundamentos de esta investigación se concluye que la metodología más acertada para la solución del problema central es la aplicabilidad de una minería de procesos basada en el Lifecycle model for process Mining que a continuación se detalla.

En la minería de procesos nos encontramos con tres apartados, el descubrimiento, la conformidad y la mejora. Así también, cada uno de estos apartados busca mejorar algún aspecto de un proceso existente y todos ellos pueden llevarse a cabo sobre el mismo proceso.

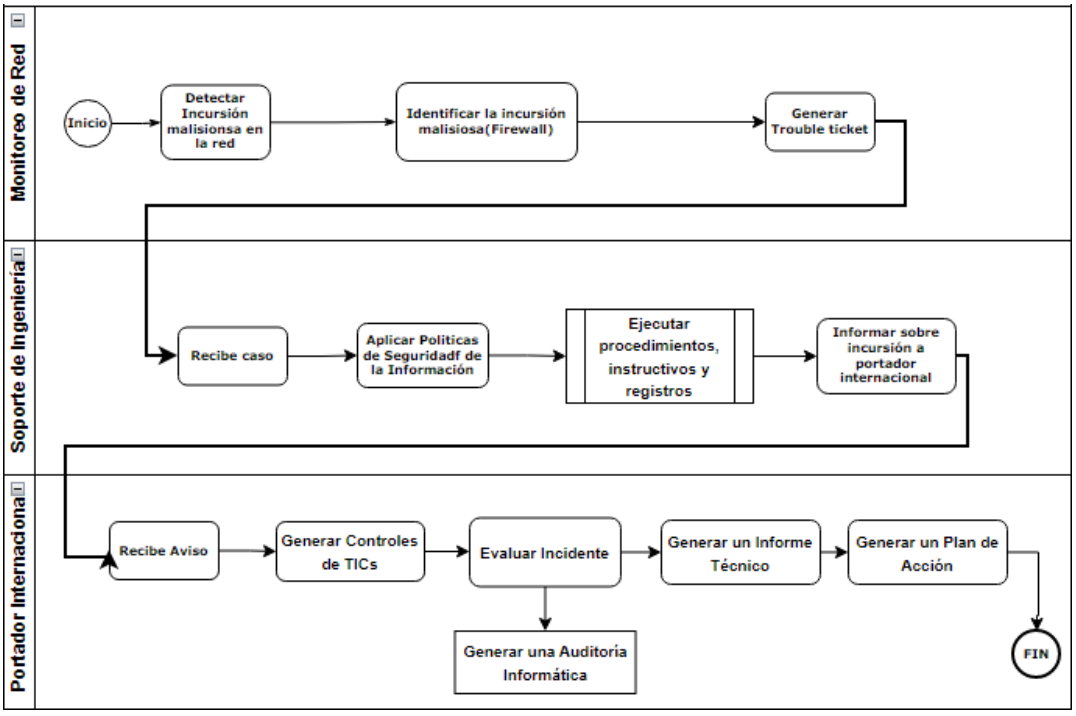
Etapa 0: Planificación y Justificación

A través de la focalización se la problematización, y enfocados en el modelo elegido para la metodología , este escenario corresponde al conocimiento total del negocio , a partir de la necesidad de la elección de dicha metodología, parte a raíz de la planeación adecuada del producto elegido para mitigar los riesgos de ciberseguridad en la empresa de internet , a partir de la adquisición del ProM justificado en su aplicabilidad y los beneficios que una minería de procesos trae al servicio de internet que se ofrece , evitando riesgos de plagio, piratería, fuga

de información y mejor de calidad y rapidez en el servicio. Del levantamiento de procesos realizado a una empresa proveedora de servicio de acceso a internet, se puede denotar que como un proceso crítico se tiene la Atención de Incidencias por Ataques Informáticos. El cual presenta actividades y tareas descritas en la gráfica expuesta a continuación. (Véase Figura 25)

Figura 25

Procesos de atención e incidencias de ataques informático



Etapa 1: Extracción de Datos

A raíz de la extracción de datos basados en los algoritmos y la información recopilada de la metodología aplicada, permite a la empresa analizar los procesos con respecto a la ciberseguridad orientados en los datos ejecutados reales provenientes de las fuentes de información. De la abstracción realizada se puede observar los principales tipos de ataques con la referencia de IPs involucradas, así como la ponderación para cada tipo de ataque. Debemos mencionar que la ponderación de cada afectación está dada por un análisis de impacto de las

misma en la red. Esta ha sido incluida para motivo de cálculo, requerido como una variable. (Véase Tabla 19)

Tabla 19

Incidentes basado en la extracción de los datos y la verificación de los 14 incidentes establecidos por ataques informáticos estipulado en (Telecomunicaciones, 2022).

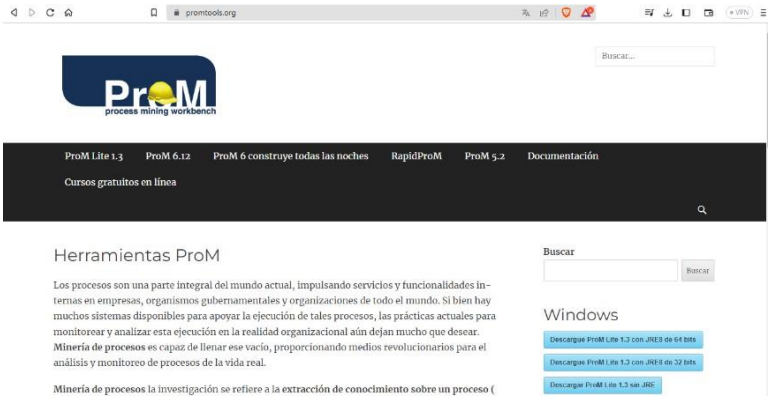
Caso ID	Tipo de Incidentes	Numeros de IPs	Puntaje
1	Sinkhole	3738	130
2	Scanners	2564	100
3	Malware	1791	100
4	Microsoft_Sinkhole	756	90
5	Bruteforce	719	90
6	Defacement	252	80
7	Spam	29	30
8	Phishing	15	90
9	Botnet	3	11
10	Información	3	70
11	SQL_Injection	1	50
12	Suplantación de Identidad	1	60
13	Comand_and_Control	1	30
14	Compromise Webside	1	35

Etapa 2: Creación de modelos de Flujo y Eventos

Para la creación del modelo de flujo del proceso, se deberá utilizar la herramienta ProM, la misma que es propuesta por un grupo de investigadores de la Universidad Técnica de Eindhoven. De esta investigación determina que esta herramienta tiene algunas ventajas respecto a otras herramientas de minería de procesos. Se trata de un framework de acceso libre, además de ello tiene algunos algoritmos para el mejoramiento, descubrimiento y análisis de procesos. A continuación, se despliega la utilización y ejecución del ProM, alineado a la metodología elegida. Las distintas versiones de la herramienta ProM están disponibles en el sitio https://promtools.org/. Para esta investigación, consideramos la versión ProM 6.12, ya que se trata de una versión de software que contiene todos los algoritmos para las simulaciones que podrían darse. (Véase Figura 26)

Figura 26

Ejecución del ProM



Nota. Elaborado por: autor basado en la aplicación y ejecución del ProM

Para ser procesado por el ProM, debe transformarse a un archivo con extensión CSV para luego volverse a transformar XES. (Véase Figura 27)

Figura 27

Transformación del archivo de extensión

Figura 28

Importación de los registros al ProM

Una vez generado el archivo en formato CSV, este debe ser importado desde el ProM. Esta lista de registros debe contener un formato adecuado para que pueda ser procesado y simulado como proceso. (Véase Figura 28 y Figura 29)

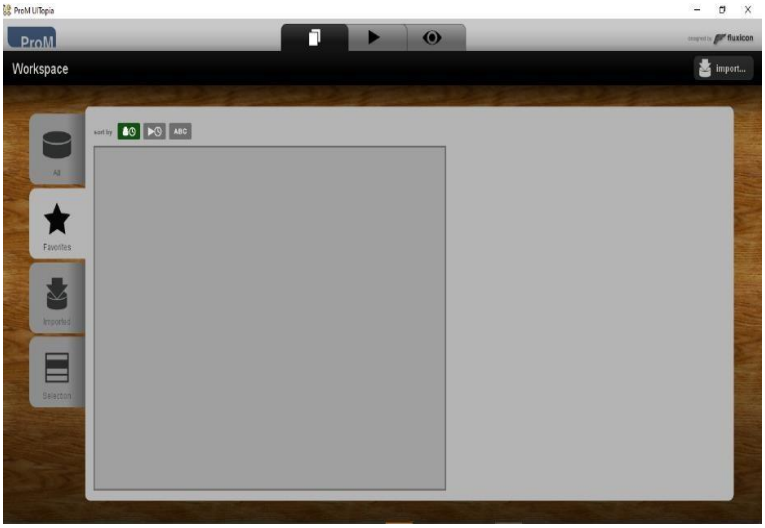
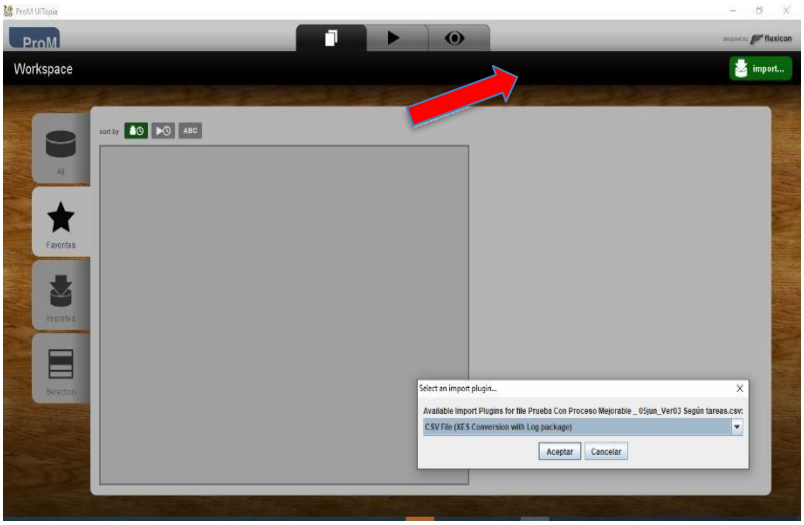


Figura 29

Finalización de la ejecución del ProM



Una vez ejecutado el ProM se evidencia, que se puede modelar y minar un proceso a partir de parámetros obtenidos. Para ello es necesario generar una lista de registros, parametrizados acorde al formato que propone la herramienta. Se debe entender que la herramienta ProM podrá procesar archivos con extensión XES. Es por ello que será necesario que será necesario convertir una lista de registro, a continuación, se presentan la data obtenida para dos casos: (Véase Tabla 20)

Tabla 20

Datos proporcionados como amenazas a través del ProM.

Caso ID	Actividad	Ponderación	Tiempo	Tiempo final
Phishing	Detectar Incursión maliciosa en la red	90	21/2/2022 13:45	21/2/2022 13:47
Phishing	Identificar la incursión maliciosa(Firewall)	90	21/2/2022 13:49	21/2/2022 13:51
Phishing	Generar Trouble ticket	90	21/2/2022 14:45	21/2/2022 14:47
Phishing	Recibe caso	90	21/2/2022 14:48	21/2/2022 14:50
Phishing	Aplicar Politicas de Seguridadf de la Información	90	21/2/2022 14:49	21/2/2022 14:51
Phishing	Ejecutar procedimientos, instructivos y registros	90	21/2/2022 14:52	21/2/2022 14:54
Phishing	Informar sobre incursión a portador internacional	90	21/2/2022 14:56	21/2/2022 14:58
Phishing	Recibe Aviso	90	21/2/2022 15:07	21/2/2022 15:09
Phishing	Generar Controles de TICs	90	21/2/2022 15:12	21/2/2022 15:14
Phishing	Evaluar Incidente	90	21/2/2022 15:16	21/2/2022 15:18
Phishing	Generar un Informe Técnico	90	21/2/2022 15:20	21/2/2022 15:22

Phishing	Generar un Plan de Acción	90	21/2/2022 15:51	21/2/2022 15:51
Sinkhole	Detectar Incursión malisionsa en la red	130	6/5/2022 13:45	6/5/2022 13:45
Sinkhole	Identificar la incursión maliciosa(Firewall)	130	6/5/2022 13:49	6/5/2022 13:49
Sinkhole	Generar Trouble ticket	130	6/5/2022 14:45	6/5/2022 14:46
Sinkhole	Recibe caso	130	6/5/2022 14:47	6/5/2022 14:48
Sinkhole	Aplicar Políticas de Seguridad de la Información	130	6/5/2022 14:49	6/5/2022 14:50
Sinkhole	Ejecutar procedimientos, instructivos y registros	130	6/5/2022 14:52	6/5/2022 14:54
Sinkhole	Informar sobre incursión a portador internacional	130	6/5/2022 14:56	6/5/2022 14:58
Sinkhole	Recibe Aviso	130	6/5/2022 15:07	6/5/2022 15:09
Sinkhole	Generar Controles de TICs	130	6/5/2022 15:12	6/5/2022 15:14
Sinkhole	Evaluar Incidente	130	6/5/2022 15:15	6/5/2022 15:16
Sinkhole	Generar un Informe Técnico	130	6/5/2022 15:17	6/5/2022 15:18
Sinkhole	Generar un Plan de Acción	130	6/5/2022 15:19	6/5/2022 15:20

Etapa 3: Creación del modelo Integrado del Proceso

Una vez importada la lista de registro y convertida a XES, se parametriza el modelado respecto a la duración de cada actividad. Sin embargo, se puede ingresar un mayor número de parámetros.

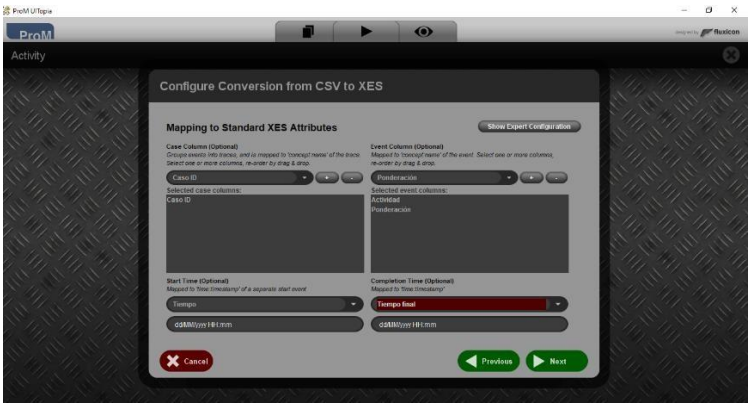
De lo mencionado anteriormente, se realizará un modelado ingresando un nuevo parámetro. Este es la ponderación por impacto del ataque en la red. (Véase Figura 30 y Figura 31)

Figura 30

Modelado del Proceso

Figura 31

Parámetros de ataque en Red

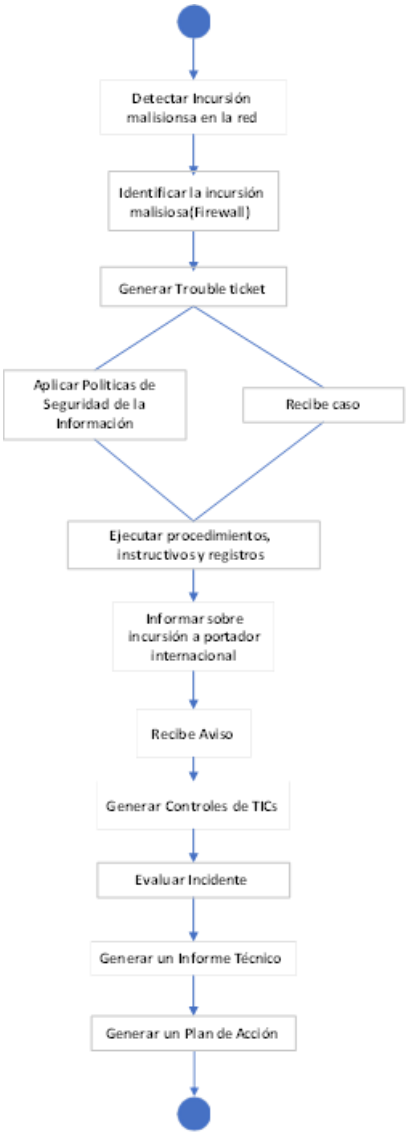


Etapa 4: Soporte Operativo

De la simulación realizada, se observa que en primera instancia se parametriza las actividades del proceso solo por tiempos, obteniendo el siguiente modelo de flujo: (Véase Figura 32)

Figura 32

Eje o Columna Vertebral del Modelado



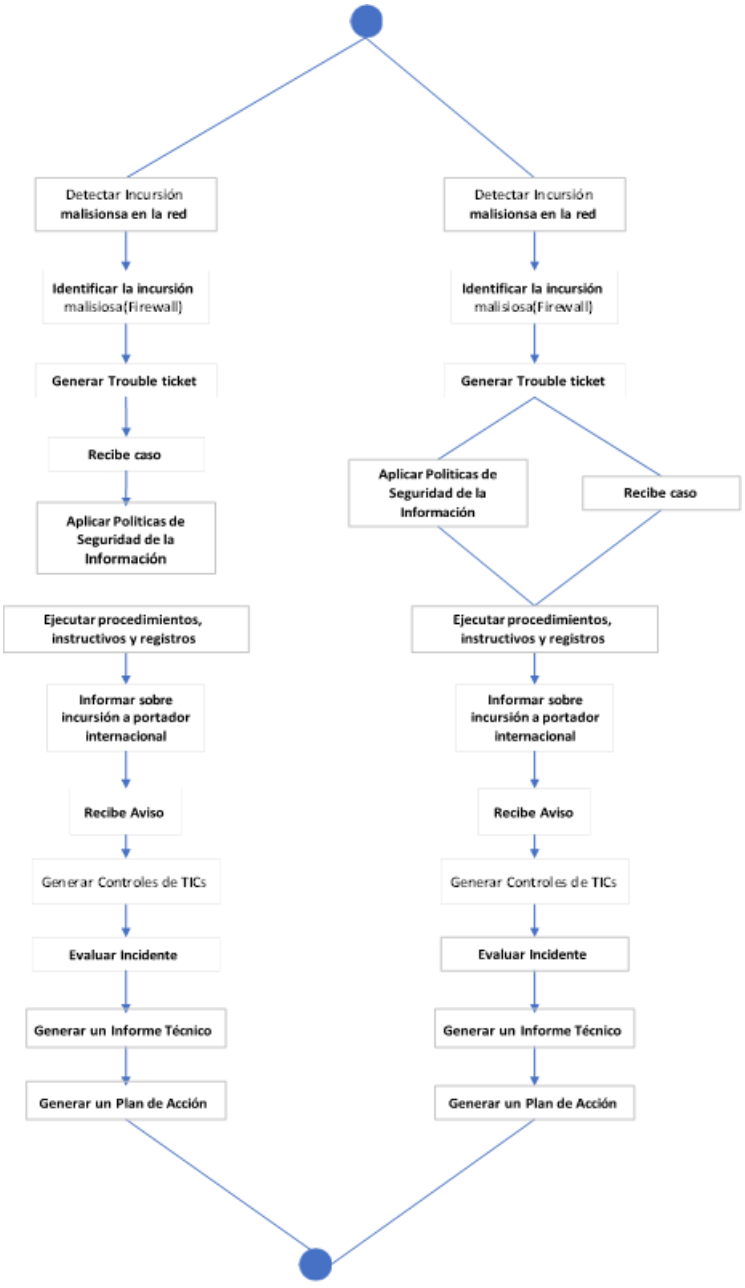
Adicional a esto, se realiza un modelado de procesos parametrizando el tiempo de cada actividad, así como la ponderación de cada caso. Esta ponderación, como ya se había comentado anteriormente; está dada por el impacto de la afectación en la red.

Se observa, que se generaron una especie de doble ramal, como cual nos indica que el camino de la izquierda es el más importante por la alta ponderación del tipo de ataque.

Debemos mencionar que para el este modelado el valor del fitness es superior a 0.8, lo cual indica que la mayoría de las tareas se cumplen. (Véase Figura 33)

Figura 33

Eje o Columna Vertebral II del Modelado



Relación con controles de la normativa ISO-27001

La Minería de Procesos parte de esta investigación está basada en controles de la norma ISO-27001, de los cuales se utilizaron criterios de buenas prácticas de seguridad informática. Los controles correlacionados con el modelado de procesos obtenidos están contenidos en categorías propuestas por el estándar, estas son las siguientes:

- Política de seguridad de la información
- Organización de la seguridad de la información
- Gestión de incidentes de seguridad de la información
- Operaciones de seguridad

CONCLUSIONES

- La herramienta para Minería de Procesos ProM, está disponible para su uso y aplicación en diferentes entornos informáticos. Sea este en las etapas de diseño, provisión e implementación de proyectos. Dada que es de uso libre facilita su accesibilidad.
- Es posible aplicar Minería de Procesos en casi todo tipo de organizaciones. Para el caso particular que organizaciones que traten con tecnologías de la información, este puede ayudar a mejorar los procesos de operación y mantenimiento.
- La herramienta utilizada permite parametrizar múltiples variables, lo cual ayuda al mejoramiento del proceso de forma ágil y precisa. Esto debido a que se lo puede manejar en un entorno gráfico.
- En nuestro entorno, la minería de procesos ha sido escasamente utilizada en la gestión de proyectos, y los casos que pueden ser detectados se refieren a casos muy particulares. Este trabajo presenta un método sistemático y adaptable, que guía el trabajo en conjunto del experto en gestión de proyectos y el experto en minería de procesos.
- Como se denota en las figuras 32 y 33, el modelo cambia de acuerdo a los caminos (path) que se quieran visualizar, en el caso de la figura 32 con una ponderación(presión) del 90, el proceso se mantiene bajo control. Mientras que para la figura 33, donde se aumenta otro caso, se denota que el de mayor ponderación (130) evita una tarea para mantener una precisión del 100%, o dicho de otra manera para mantener los procesos bajo control. Todo esto con un fitness de 0.8. Por lo expuesto, para la validación de la investigación, la comparación de paths de las figuras 32 y 33 se vuelve clave, porque al tener un modelo con un alto nivel de fitness y requerir un cumplimiento de los procesos;

se vuelve útil en la identificación de tareas y áreas a mejorar en los procesos de seguridad.

- Adicional al modelado de procesos generado por la herramienta de Process Mining, se puede considerar como un criterio adicional la armonía de las tareas con los tiempos de duración de las mismas. Según se puede observar en la Tabla 20, los tiempos de las tareas deben estar acordes a la disposición, operatividad y a la creación de infraestructura de TI. Estos criterios se vuelven un insumo para el modelador de procesos y con ello para la toma de decisiones.

Bibliografía

Aguirre Mayorga, H. (2016). Minería de procesos Fundamentos y metodología de aplicación. (E.P. Javeriana, Ed.) Editorial Pontificia Universidad Javeriana. https://doi.org/https://www.google.com.ec/books/edition/Miner%C3%ADa_de_procesos/5J4xDwAAQBAJ?hl=es&gbpv=0

Alvarado LLano , W., & Changoluisa Pachacama, I. (Julio de 2019). Repositorio UTC. Repositorio UTC: http://repositorio.utc.edu.ec/bitstream/27000/5323/1/PI-001347.pdf

Arreola García, A. (2019). Ciberseguridad. (S. V. Editores, Ed.) Siglo XXI Editores México. https://doi.org/https://www.google.com.ec/books/edition/Ciberseguridad/ZqHDDwAAQBAJ?hl=es&gbpv=0

Bakht, D. (2020). Ciberseguridad. (H. Bakht, Ed.) Humayun Bakht. https://doi.org/https://www.google.com.ec/books/edition/Ciberseguridad/1xzxDwAAQBAJ?hl=es&gbpv=0

Campos Arenas, A. (2021). Métodos mixtos de investigación. (Magisterio, Ed.) Magisterio Español. https://doi.org/https://www.google.com.ec/books/edition/M%C3%A9todos_mixtos_de_investigaci%C3%B3n/AIYqEAAAQBAJ?hl=es&gbpv=0

Carpentier, J.-F. (2016). La seguridad informática en la PYME. (E. ENI, Ed.) Ediciones ENI. https://doi.org/https://www.google.com.ec/books/edition/La_seguridad_inform%C3%A1tica_en_la_PYME/LKE5_6gzBmgC?hl=es&gbpv=0

Carvajal Palomares, F. (2016). Manual. Administración y auditoría de los servicios Web (UF1272). Certificados de profesionalidad. Administración e servicios de Internet (IFCT0509). Editorial CEP, S.L. https://doi.org/https://www.google.com.ec/books/edition/Manual_Administraci%C3%B3n_y_auditor%C3%ADa_de_l/88U-DwAAQBAJ?hl=es&gbpv=0

Chamorro Sangoquiza , D. (2019). REPOSITORIO DE LA ESPE. REPOSITORIO DE LA ESPE: https://repositorio.espe.edu.ec/bitstream/21000/21822/1/T-ESPE-042004.pdf

Denzin, N., & Lincoln,Y. (2015). Métodos de recolección y análisis de datos. https://www.google.com.ec/books/edition/M%C3%A9todos_de_recolecci%C3%B3n_y_an%C3%A1lisis_de/5pPsDwAAQBAJ?hl=es&gbpv=0

Echaiz, & Flores, L. (2021). El Aporte de la Inteligencia Artificial y las TIC Avanzadas a las Sociedades del Conocimiento.(UNESCO, Ed.) UNESCO Publishing. https://doi.org/https://www.google.com.ec/books/edition/El_Aporte_de_la_Inteligencia_Artificial/9hpPEAAAQBAJ?hl=es&gbpv=0

Giant, N. (2017). Ciberseguridad para la i-generación. Narcea Ediciones. https://doi.org/https://www.google.com.ec/books/edition/Ciberseguridad_para_la_i_generaci%C3%B3n/ZPekDwAAQBAJ?hl=es&gbpv=1

Giménez Albacete, J. (2015). Seguridad en equipos informáticos. IFCT0109. (I. Editorial, Ed.) IC Editorial. https://www.google.com.ec/books/edition/Seguridad_en_equipos_inform%C3%A1ticos_IFCT0/M1YpEAAAQBAJ?hl=es&gbpv=0

González Escobosa , C. (2016).UC3M.ES. Retrieved 2023, from https://e-archivo.uc3m.es/rest/api/core/bitstreams/391460dc-9300-46bc-a3a3-2122ec3e76f2/content

Hernández Bejarano, M. (2020). Ciclo de vida de desarrollo ágil de software seguro. (F. U. Libertadores, Ed.) Fundación Universitaria Los Libertadores. https://doi.org/https://www.google.com.ec/books/edition/Ciclo_de_vida_de_desarrollo_%C3%A1gil_de_sof/XdQ7EAAAQBAJ?hl=es&gbpv=0

Hitpass, B. (2017). BPM: Business Process Management Fundamentos y Conceptos de Implementación. (U. T. María, Ed.) Universidad Técnica Federico Santa María.

https://doi.org/https://www.google.com.ec/books/edition/BPM_Business_Process_Management/Dm4-MGAy5vMC?hl=es&gbpv=0

Joyanes, L. (2015). Sistemas de Información en la empresa. (colombia, Ed.) colombia. https://doi.org/https://www.google.com.ec/books/edition/Sistemas_de_Informaci%C3%B3n_en_la_empresa/oHNxEAAAQBAJ?hl=es-419&gbpv=0

Joyanes, L. (2021). Internet de las cosas. (A. Editorial, Ed.) Alpha Editorial. https://doi.org/https://www.google.com.ec/books/edition/Internet_de_las_cosas/t816EAAAQBAJ?hl=es&gbpv=0

Maldonado Pinto, J. (2018). Metodología de la investigación social Paradigmas: cuantitativo, sociocrítico, cualitativo, complementario. (E. d. U, Ed.) Ediciones de la U. https://doi.org/https://www.google.com.ec/books/edition/Metodolog%C3%ADa_de_la_investigaci%C3%B3n_social/FTSjDwAAQBAJ?hl=es&gbpv=0

Manterola, N., & Sondergaard, K. (2021). Responsabilidad de los buscadores de Internet y redes sociales. elDial.com. https://doi.org/https://www.google.com.ec/books/edition/Responsabilidad_de_los_buscad ores_de_Int/A0RrEAAAQBAJ?hl=es&gbpv=0

Martín Peña, M., & Díaz Garrido, E. (2016). Fundamentos de dirección de operaciones en empresas de servicios. (E. Editorial, Ed.) ESIC Editorial. https://doi.org/https://www.google.com.ec/books/edition/Fundamentos_de_direcci%C3%B3n_de_operaciones/Kc9QDAAAQBAJ?hl=es&gbpv=0

Menéndez Arantes, S. (2022). Auditoría de la Seguridad Informática. (Ra-Ma, Ed.) RA-MA Editorial. https://doi.org/https://www.google.com.ec/books/edition/Auditor%C3%ADa_de_la_Seguridad_Inform%C3%A1tica/C864EAAAQBAJ?hl=es&gbpv=0

Ortega Candel , J. (2021). Ciberseguridad. Manual práctico. (Paraninfo, Ed.) Ediciones Paraninfo S.A.

https://www.google.com.ec/books/edition/Ciberseguridad_Manual_pr%C3%A1ctico/QsROEAAAQBAJ?hl=es&gbpv=0

Peña Valenzuela, D. (2013). Responsabilidad de los proveedores del servicio de internet en relación con la propiedad intelectual. (D. P. Valenzuela, Ed.) Universidad Externado de Colombia. https://doi.org/https://www.google.com.ec/books/edition/Responsabilidad_de_los_proveedores_del_s/3dpHAQAAQBAJ?hl=es&gbpv=0

Peña Valenzuela, D. (2015). Responsabilidad de los proveedores del servicio de internet en relación con la propiedad intelectual. (E. R. García, Ed.) Universidad Externado. https://doi.org/https://www.google.com.ec/books/edition/Responsabilidad_de_los_proveedores_del_s/sTSjDwAAQBAJ?hl=es&gbpv=0

Piattini Velthuis, M., García Rubio, F., & Pino, F. (2019). Calidad de Sistemas de Información. 5ª edición ampliada y actualizada. (R.-M. S. Publicaciones, Ed.) RA-MA S.A. Editorial y Publicaciones. https://doi.org/https://www.google.com.ec/books/edition/Calidad_de_Sistemas_de_Informaci%C3%B3n_5%C2%AA/tc-4EAAAQBAJ?hl=es&gbpv=0

POSTIGO PALACIOS, A. (2020). Seguridad informática (Edición 2020). (S. Ediciones Paraninfo, Ed.) Ediciones Paraninfo, S.A. https://www.google.com.ec/books/edition/Seguridad_inform%C3%A1tica_Edici%C3%B3n_2020/UCjnDwAAQBAJ?hl=es&gbpv=0

Raya, V. (2020). Gestión de Proyectos (GRADO SUPERIOR). Grupo Editorial RA-MA. https://doi.org/https://www.google.com.ec/books/edition/Gesti%C3%B3n_de_Proyectos_GRADO_SUPERIOR/TI2fDwAAQBAJ?hl=es&gbpv=1&dq=normas+iso+27000&pg=PA29&printsec=frontcover

Rengifo García, E. (2015). Responsabilidad de los proveedores del servicio de internet en relación con la propiedad intelectual. (E. R. García, Ed.) Universidad Externado.

https://doi.org/https://www.google.com.ec/books/edition/Responsabilidad_de_los_proveedores_del_s/sTSjDwAAQBAJ?hl=es&gbpv=0

Romero Castro, M., Figueroa Morán, G., Vera Navarrete, D., Álava Cruzatty, J., & Parrales Anzúles, G. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. (3Ciencias, Ed.) 3Ciencias. https://doi.org/https://www.google.com.ec/books/edition/INTRODUCCI%C3%93N_A_LA_SEGURIDAD_INFORM%C3%81TIC/5Z9yDwAAQBAJ?hl=es&gbpv=0

Telecomunicaciones, A. d. (2022). Número de IP notificadas durante el año 2022.

Van der Aalst, W. (1998). Process Mining; Discovery, Conformance and. Londres. https://doi.org/file:///C:/Users/PERSONAL/Documents/MAESTR%C3%8DA%20BORIS%20GARAICOA/Process%20Mining_%20Discovery,%20Conformance%20and%20Enhancement%20of%20Business%20Processes%20(%20PDFDrive%20).pdf

Van der Aalst, Wil M. (2011). https://doi.org/https://www.uv.mx/iiesca/files/2018/11/12CA201801.pdf

Zarzar Charur, C. (2015). Métodos y Pensamiento Crítico 1. (L. -G. Patria, Ed.) Larousse - Grupo Editorial Patria. https://doi.org/https://www.google.com.ec/books/edition/M%C3%A9todos_y_Pensamiento_Cr%C3%ADtico_1/EtBUCwAAQBAJ?hl=es&gbpv=0